Catholic University Journal of Law and Technology

Volume 27
Issue 2 *Spring 2019*

Article 3

2019

The Department of Justice Versus Apple Inc. -- The Great Encryption Debate Between Privacy and National Security

Julia P. Eckart

THE DEPARTMENT OF JUSTICE VERSUS APPLE INC.—THE GREAT ENCRYPTION DEBATE BETWEEN PRIVACY AND NATIONAL SECURITY

*Julia P. Eckart**

For approximately forty-three days in early 2016, a very public and legally contentious dispute waged between Apple Inc. ("Apple") and the Department of Justice ("DOJ") regarding data encryption and privacy interests of electronic devices versus law enforcement and national security needs to search an iPhone.[1] Each party publicly, and through multiple court filings,[2] argued their polar

* Ms. Julia P. Eckart, USAF Civilian Attorney, B.A. Economics, Mount Holyoke College (1985); J.D., Emory University School of Law (1989). Ms. Eckart is a member of the Florida Bar. The views expressed in this article are those of the author and do not reflect the views of the United States Government, Department of Defense, or United States Air Force.

1 Elizabeth Weise, *Apple v FBI timeline: 43 days that rocked tech*, USA TODAY (Mar. 15, 2016, 6:26 PM), https://www.usatoday.com/story/tech/news/2016/03/15/apple-v-fbi-timeline/81827400.

2 *Id.* Although numerous amicus briefs were filed, this Article primarily focuses on the

positions as to the validity of a court order, issued pursuant to the All Writs Act[3] ("AWA"), requiring Apple to provide technical assistance to allow the Federal Bureau of Investigation ("FBI") to access the iPhone's encrypted data. On one hand, the DOJ argued the court's order was authorized and appropriate; on the other hand, Apple argued the court exceeded its authority when it ordered Apple to provide the described technical assistance in violation of statutory law, the separation of powers doctrine, and various provisions of the U.S. Constitution ("Constitution"). This ping-pong-like debate between the two parties made it difficult to determine what was truly required of Apple, whether it was legally appropriate, and who had the stronger legal position. In the end, the court vacated the order because the DOJ provided notice to the court that it had been able to access the iPhone.[4] However, the issue of data encryption and privacy interests of electronic devices versus national security and law enforcement's need to search electronic devices is still unresolved. This Article is an attempt to objectively examine and assess each party's legal arguments concerning the court's use of the AWA to order Apple to provide the technical assistance and identify any areas that may need further explanation before a final determination can be made.[5]

I. THE FACTS UNDERLYING THE DOJ–APPLE DISPUTE

On December 2, 2015, after pledging allegiance to Khalifa bu bkr al bhaghdadi al quraishi, a reference to Abu Bakr Al Baghdadi, leader of the Islamic State of Iraq and al-sham ("ISIS"), Syed Rizwan Farook and his wife, Tafsheen Malik Farook ("Mali"), went to the Inland Regional Center ("IRC"), his place of employment, with two assault rifles and semiautomatic handguns.[6]

---

parties' court-filed documents.

3 28 U.S.C. § 1651 (2015).

4 Order Vacating February 16, 2016 Order at 1, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate #[3]5KGD203 (C.D. Cal. Mar. 29, 2016) (No. 16-10) [hereinafter Final Order].

5 As there was no final court decision on the legal dispute before the court, this Article is based upon Apple Inc.'s (Apple's) and the Department of Justice's (DOJ's) court-filed documents and publicly available information.

6 Gov't's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search; Memorandum of Points and Authorities; Declaration of Christopher Pluhar; Exhibt Memo at 2, *In re* Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 19, 2016) (No. 16-10) [hereinafter Application]; Declaration of Christopher Pluhar at 2, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 16, 2016) (No. 16-10) [hereinafter Pluhar Declaration].

They walked into a conference room where his co-workers were attending a holiday luncheon/training session, and opened-fire, killing 14 people and injuring 22 others.[7] Malik and Farook were killed later that day in a shoot-out with law enforcement.

At the time, the December 2, 2015 attack was "the deadliest Islamic State-inspired attack on American soil,"[8] resulting in an FBI investigation. By December 3, 2015, the FBI had obtained a Search and Seizure Warrant, based upon probable cause, from Magistrate Judge David T. Bristow authorizing the FBI to search and seize a "Black Lexus IS300 California license plate #5KGD203, [35KGD203] . . . vehicle identification number JTHBD192X50094434" and various items found in the vehicle to include digital devices.[9] The subsequent FBI search located an Apple digital device, specifically an "iPhone 5C, Model: A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI: 358820052301412, on the Verizon Network"[10] ("Device").

Farook's employer, the San Bernardino County Department of Public Health ("SBCDPH"), owned the Device and provided it to him for business purposes. While the SBCDPH gave the FBI permission to search the iPhone (and permission for Apple's technical assistance), the Device was passcode protected and the SBCDPH did not know the passcode.[11] The SBCDPH also owned the Device's corresponding iCloud account, and even though the SBCDPH did not know the iCloud account password, it had the ability to reset the password.[12]

According to FBI Supervisory Special Agent ("SSA") Christopher Pluhar, the FBI found the Device powered off inside of the vehicle. When the Device was

---

7 Application, *supra* note 6; Pluhar Declaration, *supra* note 6.

8 Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES (Dec. 4, 2015), https://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

9 Application, *supra* note 6, at 1 (The majority of the court-filed documents have "35KGD203" as the license plate number versus "#5KGD203." Although it cannot be conclusively determined, this appears to be a typographical error, with the inadvertent use of the shift key when typing the number "3".).

10 *Id.*

11 Gov't's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search; Exhibit at 18 n. 7, *In re* Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 19, 2016) (No. 16-10) [hereinafter Motion to Compel]; Pluhar Declaration, *supra* note 6, at 3.

12 Motion to Compel, *supra* note 11; Supplemental Declaration of Christopher Pluhar in Support of Gov't's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 1-2, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 19, 2016) (No. 16-10) [hereinafter Pluhar Supplemental Declaration].

powered on, it displayed a four-digit pad (indicating a four-digit passcode) and was running iOS9, an operating system for Apple's mobile devices.[13] Although the SBCDPH had deployed the mobile device management system ("MDM") to manage its employee-issued iPhones, the MDM system had not been fully implemented at the time and so was not yet installed on Farook's Device.[14] The MDM system would have enabled the SBCDPH to "enroll iOS devices in an enterprise environment, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely wipe or lock managed devices."[15] Thus, had the MDM been implemented on his Device, the SBCDPH would have had the ability to clear the passcode and unlock the iPhone.[16]

The FBI faced numerous issues related to the examination of the Device. First, the FBI did not know or have access to the passcode.[17] Not only was the FBI faced with a large iteration count, it also had to manually, rather than electronically, enter the passcodes.[18] In addition, Apple's iPhone operating system ("iOS") allowed the user to implement an "'auto-erase function' that would, if enabled, result in the permanent destruction of the required encryption key material after ten erroneous attempts at the passcode."[19] The FBI had reason to believe the function was enabled as the SBCDPH stated the Device had been provided to Farook with the function enabled. In addition, the most recent examination of the device's corresponding iCloud account indicated the auto-erase function was enabled.[20] Thus, the FBI concluded it risked permanent inaccessibility to the data in the iPhone after ten erroneous passcode attempts as the auto-erase function would erase the encryption key needed to access the encrypted data.[21]

Given these concerns and the impact to its ability to access the data, the FBI

---

13 Gov't's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 1-2, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate #[3]5KGD203 (C.D. Cal. Mar. 10, 2016) (No. 16-10) [hereinafter Opposition]; Pluhar Supplemental Declaration, *supra* note 12.

14 Pluhar Supplemental Declaration, *supra* note 12.

15 *iOS Security*, *iOS9.0 or later*, APPLE INC. 1, 52 (Sept. 2015).

16 *Id*.

17 Application, *supra* note 6, at 3.

18 A large iteration count makes each passcode attempt slower. As a result, "it would take years to try all combinations of a six-character alphanumeric passcode." *Id.* at 5.; Pluhar Declaration, *supra* note 6, at 3; Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agency in Search, and Opposition to Government's Motion to Compel Assistance at 6, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 25, 2016) (No. 16-10) [hereinafter Motion to Vacate].

19 Application, *supra* note 6, at 3.

20 *Id.* at 6.

21 *Id*.

sought Apple's technical assistance to disable certain non-encrypted security features within the device's operating system.[22] The FBI first sought Apple's voluntary technical assistance, which was provided on a limited basis; however, Apple denied the FBI's request to disable various non-encrypted security features[23] and/or refused to discuss disabling the non-encryption security features[24] which led to this public and legally contentious dispute between Apple and the DOJ.

A. Timeline of the Parties' Court-Filed Documents

Subsequent to Apple's denial to voluntarily disable the non-encryption features, the DOJ filed the Government's Ex Parte Application for Order Compelling Apple Inc. to Assist Agents in Search ("Application") on February 16, 2016 with the United States District Court for the Central District of California. The Application included SSA Pluhar's Declaration and the court-issued search warrant relied upon by the FBI. The Application requested the court to order Apple, pursuant to the AWA,[25] to provide technical assistance to the FBI to access the Device's encrypted data.[26]

That same day, Magistrate Judge Sherri Pym signed the Order Compelling Apple, Inc. to Assist Agents in Search ("Order"). The Order required Apple to provide reasonable technical assistance such that it would accomplish the following:

> (1) Disable the auto-erase function whether it was enabled or not;
> (2) Allow the FBI to electronically submit passcodes (via some other physical device port, Bluetooth, Wi-Fi, or any other protocol available on the device); and
> (3) Permit the FBI to enter passcodes in a manner such that the software would not intentionally add delay times between passcodes attempts beyond that which is incurred by Apple hardware.[27]

The Order also included the DOJ's proposed course of action demanding Apple provide the FBI a custom signed iPhone Software ("IPSW") file, and a recovery bundle or some other Software Image File ("SIF") that could be loaded on the

---

22 *Id.*
23 *Id.* at 5.
24 Opposition, *supra* note 13, at 21.
25 28 U.S.C. § 1651 (2015).
26 Application, *supra* note 6, at 1.
27 Order Compelling Apple, Inc. to Assist Agents in Search at 2, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 16, 2016) (No. 15-0451M) [hereinafter Order].

device. The SIF would load and run from Random Access Memory ("RAM") so that the device would remain forensically sound. Per the DOJ, because the SIF would create a unique identifier, it would only load and run on the device. The SIF would bypass the auto-erase function; allow the FBI to input passcodes electronically; and remove various time delays.[28] The SIF could be installed at a government facility or an Apple facility; however, a government representative would electronically enter the passcodes.[29] Apple was ordered to provide the DOJ Apple's reasonable costs for the technical assistance.[30] Finally, the Order gave Apple the flexibility to develop other options for achieving the FBI's stated goals, subject to the DOJ's agreement.[31]

In response to the Order, Tim Cook, Apple's Chief Executive Officer, published an on-line notice entitled, A Message to Our Customers ("Message") where Apple indicated it would legally challenge the Order's validity, and outlined its policy reasons for challenging the United States Governments ("Government's") actions.[32]

On February 19, 2016, the DOJ filed the Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search ("Motion to Compel").[33] Apple's Message was an exhibit to the Motion to Compel. Then, on February 25, 2016, Apple filed Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Government's Motion to Compel Assistance ("Motion to Vacate").[34] Apple also filed two Declarations, one signed by Erik Neuenschwander, Manager of User Privacy,[35] and one signed by Lisa Olle, Manager of Global Privacy & Law Enforcement Compliance Team.[36]

---

28 *Id*.

29 *Id*. at 2-3.

30 *Id*. at 3.

31 *Id*.

32 Tim Cook, *A Message to Our Customers*, APPLE INC. (Feb. 16, 2016), http://www.apple.com/customer-letter.

33 Weise, *supra* note 1.

34 *Id*.

35 As the manager of User Privacy, Erik Neuenschwander is "responsible for the privacy design of Apple's products and services" and provides many of the technical details about the Device. *See* Declaration of Erik Neuenschwander in Support of Apple's Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search, and Opposition to Government's Motion to Compel Assistance at 3-4, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 25, 2016) (No. 16-10) [hereinafter Neuenschwander Declaration].

36 Lisa Olle is responsible for Apple's compliance with legal requests from international, federal, state and local law enforcement agencies; she was also responsible for Apple's response to the legal requests for information concerning the Device at issue. *See* Declaration of Lisa Olle in Support of Apple's Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search and Opposition to Gov't's Motion to Compel

In response to the Motion to Vacate, the DOJ filed the Government's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order ("Opposition").[37] The DOJ attached Declarations to the Opposition signed by SSA Pluhar,[38] Stacey Perino (a FBI Electronics Engineer),[39] and Assistant U.S. Attorney Tracy Wilkison (concerning accuracy of DOJ's submitted exhibits).[40]

On March 15, 2016, Apple filed Apple Inc.'s Reply to Government's Opposition to Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Asist Agents in Search ("Reply").[41] Apple also filed additional Declarations signed by Nicola Hanna (concerning accuracy of Apple's submitted exhibits),[42] Craig Federighi, Senior Vice President of Software Engineering, Robert Ferrini,[43] Senior Director of Worldwide Advertising & Planning, and Erik Neuenschwander.[44]

B. Issues Presented in the DOJ- Apple Litigation

After reviewing the court-filed documents, it is reasonable to assume that the DOJ did not foresee the issues that would arise in this case, including the court's authority to issue the Order pursuant to the AWA. However, Apple raised a number of complex, and to an extent, overlapping issues. Between the parties' respective positions outlined in the court documents, the dispute presents the

---

Assistance at 2, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 25, 2016) (No. 16-10) [hereinafter Olle Declaration].

37 Weise, *supra* note 1.

38 Pluhar Supplemental Declaration, *supra* note 12, at 1.

39 Declaration of Stacey Perino in Support of Gov't's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 1, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate #[3]5KGD203 (C.D. Cal. Mar. 10, 2016) (No. 16-10) [hereinafter Perino Declaration].

40 Supplemental Declaration of Tracy Wilkinson in Support of Gov't's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 1, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate #[3]5KGD203 (C.D. Cal. Mar. 10, 2016) (No. 16-10) [hereinafter Wilkinson Supplemental Declaration].

41 Weise, *supra* note 1.

42 Apple Inc.'s Reply to Government's Opposition to Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist Agents in Search at 1-2, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Mar. 15, 2016) (No. 16-10) [hereinafter Reply].

43 *Id.*

44 *Id.*

following issues:

(1) Does this case pertain to a single iPhone or all iPhones?
(2) Does the Order compel Apple to create a universal master key or back door or require Apple to hack its own customers?
(3) Did the court exceed its jurisdictional authority when it issued the Order pursuant the AWA?
(4) Did the court appropriately use the AWA when it ordered Apple to provide the mandated technical assistance?
(5) Does the Order violate Apple's First Amendment rights?
(6) Does the Order implicate anyone's Fourth Amendments rights?
(7) Does the Order violate an individual's or individuals' right to privacy?
(8) Does the Order violate Apple's Fifth Amendment rights?

However, before examining these issues, one must first have an understanding of Apple's iOS, including aspects of its architectural hardware, software and data encryption, and non-encryption security features.

II. APPLE'S IOS9.0 SECURITY GUIDE

The Device in this case operated on iOS9.0, Apple's iOS Security, iOS9.0 or later[45] guidebook ("iOS9.0 Security Guide") will be used as a reference of the device's encryption and non-encryption security features.[46] Based upon the review of Apple's iOS9.0 Security Guide, it is clear Apple is extremely concerned with the security lifecycle of all of its manufactured devices. Apple states, "[e]very iOS device combines software, hardware, and services [that are] designed to work together for maximum security . . . iOS protects not only the device and its data at rest, but the entire ecosystem, including everything users do locally, on networks, and with key Internet services."[47] The encryption and non-encryption security features built into all levels of Apple's devices, e.g., the hardware, firmware, software, processes, updates, apps, etc. are consistent with Apple's mission to protect its users' privacy.

A. Some of Apple's Encryption and Non-Encryption Security Features

One of Apple's encryption features, "Data Protection," is designed to protect data stored in the flash memory of the iPhone[48] which ensures a high level of

---

45 *iOS9.0 Security Guide,* APPLE INC. 1, 1 (2015).

46 Motion to Vacate, *supra* note 18 (beginning with iOS8, Apple began to incorporate passcodes into its encryption systems).

47 *iOS9.0 Security Guide, supra* note 45, at 4.

48 *See* Jeff Tyson, *How Flash Memory Works*, HOWSTUFFWORKS, https://computer.howstuffworks.com/flash-memory.htm (last visited Mar. 24, 2019) (explaining data is

encryption of the user's data. When the user sets up the iPhone's passcode, the Data Protection encryption feature is automatically enabled, and the user's data, including the user's Messages, Mail, Calendar, Contacts, Photos, Health Data are automatically encrypted.[49] The data is encrypted through a combination of a user-determined passcode (either a four to six numeric combination or a six alphanumeric combination) and a unique 256-bit Advanced Encryption Standard ("AES") key, referred to as the Unique ID ("UID"). The UID/AES 256-bit key is fused into an iPhone during its manufacture and neither Apple nor its suppliers know the UID/AES 256-bit key nor can the iPhones' software or firmware read the UID.[50] Upon set up, the user's passcode becomes entangled with the iPhone's UID; thus the stronger the passcode, the stronger the encryption key.[51] Finally, because the passcode becomes entangled with the UID, brute force attempts can only be manually entered into the iPhone.[52]

One of Apple's non-encryption security features, the large iteration count, also discourages brute force attempts on iOS9.0 as each subsequent passcode entered into the device is slowed, ensuring that it would take five to six years to try all combinations of a six-character alphanumeric passcode (using upper and lower case letters). The iteration count is calibrated so that one attempt takes approximately 80 milliseconds. As a result of the increased computational burden after each unsuccessful attempt, each subsequent passcode entry to access the iPhone becomes slower as the computational burden for each entry is increased after each attempt.[53]

Another non-encryption security feature which discourages brute force attempts is escalating time delays between incorrect passcode entries. For the first four attempts, there would be no time delay; however, for the fifth attempt there would be a 1-minute delay, for the sixth attempt, a 5-minute delay, for the seventh and eighth attempt, a 15-minute delay, and a 1-hour delay after the ninth attempt.[54] In addition, after a certain number of incorrect attempts, the time delay is set to an infinite value that results in the device not accepting any more

---

stored electronically as opposed to being stored in a computer hard drive).

49 *iOS9.0 Security Guide*, *supra* note 45, at 11-12.

50 *See id.* at 10-12; Motion to Vacate, *supra* note 18; Pluhar Declaration, *supra* note 6, at 5.

51 *See iOS9.0 Security Guide*, *supra* note 45, at 12; *see also* Motion to Vacate, *supra* note 18, at 6; Neuenschwander Declaration, *supra* note 35.

52 *iOS9.0 Security Guide*, *supra* note 45, at 12; *see also* Neuenschwander Declaration, *supra* note 35.

53 Motion to Vacate, *supra* note 18; *see also* Neuenschwander Declaration, *supra* note 35.

54 *iOS9.0 Security Guide*, *supra* note 45, at 12; *see also* Neuenschwander Declaration, *supra* note 35, at 6.

passcodes, thereby making the data permanently inaccessible.[55]

Finally, Apple has installed an auto-erase feature, called "Erase Data," which if activated would delete encrypted data after ten consecutive, incorrect passcode entries.[56] This setting is also available as an administrative policy through the MDM.[57]

B. Other Hardware and Software System Security Features

According to Apple's iOS9.0 Security Guide, everything within Apple's iOS is designed to ensure only authorized/signed Apple products, processes, code, devices etc. can operate on Apple's iOS. From the initial booting of the device (e.g. beginning with the Apple root certificate) to software upgrades to apps loaded on the device, there is some level of verification and/or trust certification to ensure the security of the electronic device. Because only Apple products can run Apple's iOS and only Apple-signed code can run on Apple devices, only Apple can prevent any downgrading to an iOS through a process called System Software Authorization.[58]

Apple is able to prevent the downgrading of its iOS through the procedures required for updates to its devices. For example, during an iOS update, the device will connect to an "Apple installation authorization server and sends it a list of cryptographic measurements for each part of the installation bundle to be installed (for example, LLB, iBoot, the kernel, and OS image), a random anti-reply value (nonce), and the device's unique ID ECID."[59] It is important to note the unique ID ECID is different from the UID, the 256-bit AES Key. The ECID is a 64-bit AES key tied to a particular model[60] (e.g. an iPhone model) while the 256-bit AES Key is particular to each individual device. To prevent the downgrade, Apple's authorization server will check:

> the presented list of measurements against versions for which installation is permitted and, if it finds a match, adds the ECID to the measurement and signs the results. The server passes a complete set of signed data to the device as part of the upgrade process. Adding the ECID 'personalizes' the authorization for the requesting device . . . These steps ensure that the authorization is for a specific device and that an old iOS version form one device can't be copied to

---

55 Neuenschwander Declaration, *supra* note 35, at 4.

56 *See* Motion to Vacate, *supra* note 18 (stating the position of the DOJ that it deletes the encryption key making the data inaccessible).

57 *iOS9.0 Security Guide*, *supra* note 45, at 12; *see also* Neuenschwander Declaration, *supra* note 35, at 4.

58 *iOS Security*, *iOS9.0 or later*, *supra* note 15, at 6.

59 *Id.*

60 *Id.* at 58.

> another. The nonce prevents an attacker from saving the server's response and using it to tamper with a device or otherwise alter the software system.[61]

Overall, Apple and the DOJ agree upon the fundamental encryption and non-encryption security features articulated in Apple's iOS9.0 Security Guide. Apple and the DOJ also agree on the following matters regarding the impact the trust certification steps have on iPhones: only Apple devices can run Apple's iOS; only Apple-signed code can run on Apple devices; and one cannot downgrade the iOS. The parties are in disagreement over the Order's impact to Apple's iOS and whether those changes are personalized to only one device.[62]

III. DOES THIS CASE PERTAIN TO A SINGLE IPHONE OR ALL IPHONES?

The DOJ consistently argues this case is about a single iPhone and that it is the iPhone specifically described in the Order. Apple strongly disagrees with the DOJ's position. In fact, Apple's first sentence in its Motion to Vacate is "[t]his is not a case about one isolated iPhone."[63] Apple consistently argues what the government is mandating through the Order will significantly impact millions of Apple iPhones. Which party is correct? The answer is both, depending on one's perspective; however, while each perspective may be reasonable, one must examine that perspective according to the law in order to determine its validity.

A. DOJ's Position–It is About One, Single iPhone

Through the Order filed pursuant to the AWA and the government's Application, the DOJ informed the court that the FBI had obtained a specific device via a valid search warrant.[64] The Application also informed the court that although Apple had provided some assistance to the FBI (e.g., complied with valid subpoenas for account information, participated in telephone calls), Apple declined to voluntarily assist them in disabling various security features, resulting in its need for the Order. As written, the Application pertains to a single Apple iPhone, specifically, "iPhone 5C, Model: A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI: 358820052301412, on the Verizon Network"[65]

On February 16, 2016, Magistrate Judge Sheri Pym signed the Order directing

---

61 *Id.* at 6.

62 *See infra* text accompany notes 111–126; *see also* Perino Declaration, *supra* note 39, at 17-30.

63 Motion to Vacate, *supra* note 18, at 1.

64 Final Order, *supra* note 4, at 1.

65 *Id*.

Apple to provide the FBI technical assistance, as described in the Order,[66] for one phone, identified as "a cellular telephone, Apple make: iPhone 5C, Model: A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI: 358820052301412, on the Verizon Network."[67] Thus, given the specific wording of the Application and Order, the DOJ's perspective is reasonable.

The same day the Order was signed, Apple issued its Message[68] outlining Apple's objections to the Order. Although only a DOJ exhibit, the message foretells Apple's future legal arguments that the Order would affect the privacy and security of millions of iPhones users and the Government was requiring it to create a backdoor and/or something equivalent to a master key.[69]

On February 19, 2016, the DOJ filed its Motion to Compel given Apple's "stated interest in adversarial testing of the order's legal merits, [and] . . . to provide Apple with the due process and adversarial testing it seeks."[70] In its Motion to Compel, the DOJ repeats many of its arguments outlined in its Application, primarily focusing on how the requirements of the AWA are met. The DOJ summarizes its single, isolated iPhone argument as

> the Order is tailored for and limited to this particular phone. And the Order will facilitate only the FBI's efforts to search the phone; it does not require Apple to conduct the search or access any content on the phone. Nor is compliance with the Order a threat to other users of Apple products. Apple may maintain custody of the software, destroy it after its purpose under the Order has been served, refuse to disseminate it outside of Apple, and make clear to the world that it does not apply to other devices or users without lawful court orders. As such, compliance with the Order presents no danger for any other phone.[71]

As to Apple's public position, the Order requires Apple to write code to create a backdoor, a master key or hack its own customers. The DOJ simply denies these allegations.[72]

---

66 *See supra* text accompany notes 26-31.

67 Gov't's *Ex Parte* Application for Order Compelling Apple Inc. to Assist Agents in Search at 1, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 16, 2016) (No. 15-0451M) [hereinafter Ex Parte Application].

68 Cook, *supra* note 32.

69 *Id*.

70 Memorandum of Points and Authorities at 3 n.3, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Feb. 19, 2016) (No. 16-10) [hereinafter Memorandum].

71 *Id*. at 14-15.

72 *Id*. at 2 (citing Cook, *supra* note 32).

B. Apple's Position—It is About Millions of iPhones

On February 25, 2016, Apple responded to the DOJ's Motion to Compel with its Motion to Vacate, and its first sentence was "[t]his is not a case about one isolated iPhone."[73] Apple views this case as law enforcement and national security interests versus all iPhone users' privacy and security interests.[74] And, because the privacy and security interests of all iPhone users are at stake, this case is about millions of iPhones. Apple cites numerous articles and statements where other government attorneys have filed applications for similar orders in various jurisdictions. Additionally, Apple cites state and local officials who have publicly stated they intend to follow similar procedures to search hundreds of seized iPhones obtained through standard law enforcement investigations, as opposed to only terrorism cases.[75]

Apple's perspective is reasonable. In fact, if the Order is determined to be valid under the AWA, one could anticipate law enforcement agencies pursuing this same avenue of assistance in the future. Although Apple's position is reasonable, this case's impact is no different from any other case that would impact future prosecutions and decisions. And, each future individual request for an AWA order would still require judicial supervision and while the initial order may be issued ex parte, that entity will also have the ability to challenge that order in any future case. In addition, if the underlying order is supported with a court-ordered, probable cause search warrant, there are at least two levels of judicial oversight of the government's actions.

C. DOJ's Opposition and Apple's Reply

In its March 10, 2016, Opposition, the DOJ repeated many of its arguments. The Order applies to a single iPhone, which provides flexibility for Apple; it does not compel Apple to unlock other iPhones, nor create a backdoor or a master key.[76] In fact, it requires only the development of "a narrow, targeted piece of software capable of running on just one iPhone, in the security of Apple's corporate headquarters."[77] In Apple's March 15, 2016 Reply, Apple again argued the case is not about one, single iPhone nor is it modest given the potential impact on other iPhones.[78]

In both its Motion to Vacate and its Reply, Apple argues that if the

---

73 Motion to Vacate, *supra* note 18, at 1.
74 *Id*. at 1-2.
75 *Id*. at 3, 24; Olle Declaration, *supra* note 36, at 4.
76 Opposition, *supra* note 13, at 1.
77 Reply, *supra* note 42, at 1.
78 *Id*.

Government requires this information through a court order, it is only a matter of time before foreign governments require the same assistance from Apple. Alternatively, the DOJ contends if Apple chooses to do business in another country, it voluntarily agrees to comply with that country's laws.[79] Both parties have reasonable positions. However, Apple appears to inconsistently defend the privacy and security of its clients depending on the country of its users. Apple's iOS9.0 Security Guide demonstrates Apple's commitment to privacy and security of its devices. Apple's own website also posts its belief that "privacy is a fundamental human right."[80] However, Apple has a unique way of protecting privacy and security interests in China when it places all the data on a server operated by a government-owned company, China Telecom.[81] Apple responds to the DOJ's argument with the following:

> Apple has *never* built a back door of any kind into iOS, or otherwise made data stored on the iPhone or in iCloud more technically accessible to any country's government. The government is wrong in asserting that Apple made 'special accommodations' for China, as Apple uses the same security protocols everywhere in the world and follows the same standards for responding to law enforcement requests.[82]

Most attorneys will agree words are important. Therefore, one must examine Apple's word choice of "*more technically accessible*."[83] This does not mean the Chinese government does not have access to the data on the server. Many are also skeptical of Apple's privacy position in China.[84] In addition, while Apple

---

79 Opposition, *supra* note 13, at 26.

80 *Apple products are designed to protect your privacy*, APPLE, INC., https://www.apple.com/privacy (last visited Mar. 29, 2019).

81 Opposition, *supra* note 13, at 29 (discussing Apple's response that the data is encrypted, while foreign analysts are skeptical that Apple is not required to share the data with the Chinese Government); *see* Scott Cendrowski, *Apple's recent concession in China have a pattern*, FORTUNE (Oct. 13, 2015), http://fortune.com/2015/10/13/apples-recent-concessions-in-china-have-a-pattern/ (discussing Apple's response that the data is encrypted, while foreign analysts are skeptical that Apple is not required to share the data with the Chinese Government); Hauke Johannes Gieror, *Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses*, MERICS CHINA MONITOR (Apr. 2015), https://www.merics.org/sites/default/files/2017-09/China_Monitor_22_Cybersecurity_EN.pdf.

82 Reply, *supra* note 42, at 21.

83 Cendrowski, *supra* note 81 (describing that Apple agreed to cooperate with security assessments by the Chinese government, suggesting technical accessibility by the Chinese government).

84 *See* Stephen Nellis & Cate Cadell, *Apple moves to store iCloud keys in China, raising human rights fears*, REUTERS (FEB. 24, 2018, 12:14 AM), https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060; *see generally* Cendrowski, *supra* note 81; Gieror, *supra* note 81; David Pierson, *While it defies U.S. government, Apple abides by China's orders—and reaps big rewards*, L.A. TIMES (Feb. 26, 2016, 3:00 AM), http://www.latimes.com/business/

may follow Apple's standards for processing all law enforcement requests, not all country judicial standards for issuing orders to access one's iPhone are the same.[85] Therefore, Apple may have never "made data stored on the iPhone or in iCloud more technically accessible," one cannot simply conclude a foreign government does not have access to data stored on the iPhone, or in iCloud.[86]

Overall, each party's position is reasonable; however, the DOJ has the stronger legal position as the Order applies to the single iPhone described in the Order. While Apple's position is reasonable, the fact that a particular case may impact other cases is not an earthshattering legal concept to attorneys. Each future case would still only be decided on the facts presented in that specific case and not on hypotheticals.[87] For there is "[n]o principle . . . more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies."[88] It is also logical that if this Order is determined to be valid under the AWA, other applications would be made in the future. However, the issuance of a future order via the AWA would still be subject to judicial scrutiny and the opportunity to challenge that particular order would still exist.

IV. DOES THE ORDER COMPEL APPLE TO CREATE A BACKDOOR, A MASTER KEY OR SOMETHING EQUIVALENT TO A MASTER KEY, AND IF SO, WHAT ARE THE IMPLICATIONS?

The DOJ and Apple have polar answers as to whether Apple is required to create a backdoor. Apple argues the Order requires it to create a backdoor or something equivalent to a master key to its iOS. As firmly as Apple is set in its position, so is the DOJ in its belief that Apple is not required to create a backdoor and/or master key. What is interesting about each party's position is that neither entity provides a definition for a backdoor, nor a master key in their respective motions, and appear to argue from each party's own understanding of the terms but not conclusively known to the other.[89]

In attempting to answer the question presented, the definitions of the terms

---

technology/la-fi-apple-china-20160226-story.html; Heather Timmons, *Apple is reportedly giving the Chinese government access to its devices for "security checks"*, QUARTZ (Jan. 23, 2015), https://qz.com/332059/apple-is-reportedly-giving-the-chinese-government-access-to-its-devices-for-a-SECURITY-assessment.

85 Yoko Kubota, *Apple's China Lesson: Think Different, But Not Too Different*, WALL STREET JOURNAL (Feb. 26, 2018, 6:01 AM), https://www.wsj.com/articles/apples-china-lesson-think-different-but-not-too-different-1519642914.

86 Reply, *supra* note 42, at 21.

87 *See generally* Clapper v. Amnesty Int'l, 568 U.S. 398, 412 (2013).

88 *See id.* at 408.

89 *See generally* Motion to Compel, *supra* note 11; Motion to Vacate, *supra* note 18.

required in order to determine the Order's impact to Apple's iOS should be considered. However, there does not seem to be a universally accepted definition of backdoor in the digital world. In fact, the North Atlantic Treaty Organization Cooperative Cyber Defense Center of Excellence does not even have a definition for backdoor.[90] Rather, there are various definitions of backdoor which have developed over time,[91] with a common understanding that a backdoor in the digital world describes the means of bypassing a computer system's security protocols in order to access the computer system.[92]

The term master key seems to have a more accepted definition. For example, the *Encyclopedia of Cryptography and Security* defines master key as a cryptographic key "whose sole purpose is to protect other keys."[93] Its application is a

> cryptographic key (typically a symmetric key) . . . whose sole purpose is to protect other keys, such as session keys, while those keys are in storage, in use, or in transit. This protection may take one of two forms: the master keys, may be used to encrypt the other keys, or the master key may be used to generate other keys.[94]

Thus, the question presented becomes whether Apple's modifications to iOS (what Apple calls Gov's[95] and the DOJ calls SIF[96]) allow the DOJ the ability to access the encrypted data on this one, single iPhone through a backdoor and/or equivalent to a master key for all other iPhones (requiring no changes to GovtOS/SIF); or would the new GovtOS/SIF have to be modified to unlock another iPhone, be it the same model or different models, and what is the extent

---

90 *See* Kim Zetter, *HACKER LEXICON: WHAT IS A BACKDOOR?*, WIRED (Dec. 11, 2014, 6:35AM), https://www.wired.com/2014/12/hacker-lexicon-backdoor.

91 Back door can be defined as a "general term describing a mechanism or access point in a communications device or network that enables. the creator of software or hardware with access to date without the permission or knowledge of the user." Stephanie K. Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix-Doctrine to Follow*, 14 N.C. J. OF LAW & TECH. 489, 532 (2013); Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 460 (2012); Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the 2.0 Era*, 8 J. ON TELECOMM. & HIGH TECH L. 359, 399-400 (2010) (providing an example of FBI creating a software, "Magic Lantern" tool to steal information from suspect's computers without a warrant).

92 *See* Encyclopedia, *Backdoor Definition*, A DICTIONARY OF COMPUTER, http://www.encyclopedia.com/computing/dictionaries-thesauruses-pictures-and-press-releases/backdoor (last visited Mar. 25, 2019); Margaret Rouse, *Backdoor Definition (computing)*, TECHTARGET, http://searchsecurity.techtarget.com/definition/back-door (last visited Mar. 25, 2019); Jonathon Zdziarski, *Backdoor, A Technical Definition*, ZDZIARSKI'S BLOG OF THINGS (Jan. 13, 2017), https://www.zdziarski.com/blog/?p=6077 (discussing the need for a common understanding of backdoor in a digital world); Zetter, *supra* note 90.

93 *Master Key*, ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY (2d ed. 2005).

94 *Id*.

95 *See* Neuenschwander Declaration, *supra* note 35, at 4.

96 *See* Application, *supra* note 6, at 7.

of those modifications? If those modifications are minor, is this two steps away from a backdoor or "equivalent to a master key?"[97]

A. DOJ's Position–There Is No Mandate to Create a Backdoor or a Master Key

The DOJ preemptively filed its Motion To Compel given Apple's public position that it would legally challenge the Order.[98] In its motion, the DOJ repeats many of its arguments outlined in its Application. The primary focus of this motion is how the requirements authorizing third party assistance via the AWA, which are outlined in *United States v. New York. Telephone Co.*[99] ("N.Y. Telephone Co."), have been met. The DOJ strongly denies Apple's allegation that the Order requires Apple to write code to create a backdoor or a master key, or hack its own customers. More specifically, the DOJ argues the Order does not provide hackers and criminals access to all iPhones, nor does it require Apple to search or access the device or hack or decrypt its customers' iPhones. It also does not compromise the security of personal information of Apple products; and "does not give the government 'the power to reach into anyone's device' without a warrant or court authorization . . . [nor] does [it] compromise the security of personal information."[100] The Order allows Apple to maintain or destroy GovtOS/SIF (for the Government never needs to possess GovtOS/SIF),[101] and gives Apple flexibility to develop other options. In sum, "compliance with the Order presents no danger for any other phone and is not 'the equivalent of a master key, capable of opening hundreds of millions or locks.'"[102]

While the DOJ denies Apple's allegations in its motion, the DOJ fails to provide an explanation as to how the newly written code to disable the non-encryption security features is not a backdoor or a master key to Apple's iOS. At this point in the litigation, this is a flaw in the DOJ's position and one that must be addressed in this case and in future cases.

---

97 Motion to Compel, *supra* note 11, at 14; Motion to Vacate, *supra* note 18, at 7.

98 Motion to Compel, *supra* note 11, at 3 n.3 (This article does not examine the DOJ's preemptive filing).

99 United States v. N.Y. Tel. Co., 434 U.S. 159, 169 (1977).

100 Krishnadev Calamur, *Apple vs. the FBI: The Justice Department Fires Back*, THE ATLANTIC (Feb. 19, 2016), https://www.theatlantic.com/national/archive/2016/02/apple-fbi-san-bernardino/470169/.

101 Motion to Compel, *supra* note 11.

102 *Id.* at 15.

B. Apple's Position–It is a Mandate to Create a Backdoor and/or a Master Key

In its Motion to Vacate, Apple argues "[t]he government demands that Apple create a back door to defeat the encryption on the iPhone"[103] and "[t]he order demanded by the government compels Apple to create a new operating system—effectively a 'back door' to the iPhone—that Apple believes is too dangerous to build."[104] The focus is on Apple's choice of words to describe the Government's actions, e.g. requiring it to create a backdoor,[105] effectively create a backdoor,[106] or something equivalent to a master key.[107] However, because Apple does not provide a definition of backdoor or master key, one cannot conclusively evaluate its position. In addition, Apple's use of phrases "effectively create a back door" or "equivalent to a master key," gives Apple flexibility to maneuver around the terms "backdoor" and "master key". In other words, Apple is not required to meet a definition, yet may still obtain the benefits of the negative inference of the terms.

Apple also argues that it not only needs to write new code, but also disable existing code in order to remove the non-encryption security features and add a capability to the new iOS (GovtOS/SIF) so that passcodes can be electronically inputted into the device.[108] Thus, creating a new software system designed to defeat Apple's security features.[109] However, Apple fails to fully address whether GovtOS/SIF will work only on this particular device or whether it requires some modification to work on the same iPhone model and/or all iPhones, and if so, how significant will the modification need to be in order for it to work on the same iPhone model and/or all iPhones.

This failure to explain whether GovtOS/SIF will require any modification, and the extent of any such modification, is a potential flaw for Apple. As Mr. Neuenschwander implies, some modification to GovtOS/SIF would need to be made so that it can be used on other iPhones. He states,

> if Apple receives three orders a week similar to the one here from around the United States, the entire process described above—writing, validating, executing, and then completely destroying the code—will have to happen three times every week, week in and week out. *Each such commissioned operating system will need to be tailored to the specific combination of hardware and operating system running on the relevant device*.[110] [Emphasis added.]

---

103 Motion to Vacate, *supra* note 18, at 1.
104 *Id.* at 2.
105 *Id.*
106 *Id.*
107 *Id.* at 3.
108 *Id.* at 12.
109 *Id.* at 2, 13.
110 *See* Neuenschwander Declaration, *supra* note 35, at 10.

To what extent does Apple have to tailor GovtOS/SIF to run on another relevant device? What is a relevant device? These are unknowns that must become known as they are critical to answering the question of whether Apple is being required to create a backdoor or something equivalent to a master key, i.e., is GovtOS/SIF two-steps away from a backdoor or master key?

C. DOJ's Opposition Position

In its March 10, 2016 Opposition, the DOJ's position remained the same: the Order is written to "produce a narrow, targeted piece of software capable of running on just one iPhone, in the security of Apple's corporate HQs."[111] More importantly, the DOJ explains how a master key or backdoor cannot be created, something it failed to address in its Motion to Compel. According to the DOJ, GovtOS/SIF can only be used on the one device, and is not a master key because:

> [t]he software 'will be coded by Apple with a unique identifier of the phone so that the [software] would only load and execute on the [ ] DEVICE.' . . . A 'unique ID (ECID)' associated with each physical iPhone is incorporated into the phone's operating system. 'Adding the ECID 'personalizes' the authorization for the requesting device.' Apple has designed its phones so that every operating system must pair with the phone's ECID. ([Declarations] describing how the Apple server 'adds the ECID' before it 'signs' the iOS to be used for the upgrade.) The operating system and ECID must correspond for the operating system to work. The ordered software [GovtOS/SIF] would rely upon the same limitation.[112]

The DOJ also argues GovtOS/SIF could not be modified to run on other iPhones as GovtOS/SIF would not be released to the government or anyone else; and even "if the code were modified to run on a phone with a different ECID, it would lack a valid digital signature. Without that signature, the code would not run at all on *any* iOS phone with intact security."[113] To support its statement, the DOJ included Stacey Perino's Declaration[114] which outlines the DOJ's technical explanation as to why GovtOS/SIF would only work on a specific device. Mr. Perino's explanation relies heavily upon the ECID, a device's unique ID. According to Mr. Perino, "[t]he ECID is a unique, device-specific identifier programmed in the phone hardware during manufacture. ECID [is defined] as 'a 64-bit identifier that's unique to the processor in each iOS device. Used as

---

111 Opposition, *supra* note 13, at 1.
112 *Id*. at 25.
113 *Id*. at 29.
114 An Electronics Engineer with the FBI.

part of the personalization process, it's not considered a secret.'"[115] In its March 15, 2016 Reply, Apple states that "Mr. Perino's characterization of Apple's process . . . is inaccurate."[116] However, before addressing Apple's Reply, one must examine Mr. Perino's explanation of Apple's process.

According to Mr. Perino, when a device requires an iOS update, it connects to an approved conduit (e.g., iTunes) and provides certain information to the conduit including the device's ECID, a nonce[117] and other cryptographic measurements. The conduit then forwards this information to an Apple server where it builds a software package, e.g. the iOS update, and digitally signs it using its private key. The public key is in the device's Read Only Memory. The digital signature includes the ECID, the nonce and the cryptographic measurements originally received from the device. When the device receives the returned package (via the conduit), the device verifies the digital signature to ensure that the package is meant for that device (comparing the ECID, nonce and other cryptographic measurements sent to that received). Thus, the device is able to determine whether an older iOS system is being loaded and would not load the package if it were an older system.[118]

Mr. Perino then discusses Apple's code signing process of including the ECID into the digital signature to the device in issue. If the iOS update process occurs as described in the preceding paragraph, "the [GovtOS/]SIF could incorporate the ECID of the Subject Device, and then be signed by Apple . . . [I]f the ECID of the [GovtOS/]SIF were changed to the ECID of another device, the signature check would fail and an Apple device would not load the code."[119] Therefore, the GovtOS/SIF directed in the Order can run only on the specific device; and its creation, "tailored and signed with the unique identifier of the Subject Device, [the ECID] would not undermine the security of other iPhones that also require Apple-signed code, because each iPhone has its own unique identifier."[120] Although Mr. Perino explains that the GovtOS/SIF will load on only one device, there appears to be least one issue with his explanation, and that is the ECID is not limited to a single, specific device.

The ECID, the 64-bit identifier *that is unique to the processor* in each iOS device, referred to as the device's unique ID in the Perino Declaration as well as in Apple's iOS9.0 Security Guide [121] is not the same as the device's unique ID ("UID"), the 256-bit key that is fused into the individual device during the manufacturing process (not known to Apple, its suppliers or even the

---

115 *See iOS9.0 Security Guide*, *supra* note 45, at 58.
116 Reply, *supra* note 42, at 19.
117 A random, one-time-use value. *See iOS9.0 Security Guide*, *supra* note 45, at 6.
118 *See id.* at 10-12.
119 *See id.* at 6.
120 *Id.* at 13.
121 *Id.* at 6.

software/firmware within the device) and ultimately becoming entangled with the passcode.[122] The confusion may have occurred because Apple uses the term unique ID with the ECID as well as unique ID ("UID") to describe the 256-bit AES encryption key in its *iOS9.0 Security Guide*. Apple also uses the term "personalizes" (or "personalization") with the term "ECID"[123] which implies the ECID is unique/personal to the individual device. However, the ECID is unique to the processer in each iOS device, and thus would be unique to the processers within the same iPhone model.[124]

D. Apple's Reply to the DOJ's Opposition

In Apple's Reply, it disputes the DOJ's explanation as to why GovtOS/SIF will only run on the single device and argues GovtOS/SIF could be modified to run on other phones.[125] Mr. Neuenschwander also explains why Mr. Perino's iOS update explanation is inaccurate.

> Each time Apple releases a new operating system, that operating system is the same for every device of a *given model*. The operating system then gets a personalized signature specific to each device. This personalization occurs as part of the installation process after the iOS is created.
> *Once GovtOS[/SIF] is created, personalizing it to a new device becomes a simple process.* If Apple were forced to create GovtOS[/SIF] for installation on the device at issue in this case, it would likely take only minutes for Apple, or a malicious actor with sufficient access, to perform the necessary engineering work to install it on another device of the same model.[126] [Emphasis added.]

The critical question is then, how slight or significant the modification is such that GovtOS/SIF can be installed on another device. While Apple states it would only be minutes, thus implying little modification is required, it is unknown precisely what modifications are required. It is also unclear as to whether the modification is limited to specific models, such as "5Cs" or is broader and would include all model "5s."

---

122 *See id*.at 10.
123 *Id.* at 6.
124 *See id.*
125 Reply, *supra* note 42, at 19; Supplemental Declaration of Erik Neuenschwander in Support of Apple Inc.'s Reply in Support of Motion to Vacate Order Compelling apple Inc. to Assist Agency in Search at 6, *In re* the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203 (C.D. Cal. Mar. 15, 2016) (No. 16-10) [hereinafter Neuenschwander Supplemental Declaration].
126 Neuenschwander Supplemental Declaration, *supra* note 125.

Apple uses phrases "equivalent to a master key," "create a back door" or "in effect, create a back door."[127] Given the definition of master key,[128] if some modification is required, Apple has not been ordered to create a master key for all its iPhones; however, Apple uses terms "equivalent to a master key,"[129] thereby allowing Apple to argue the negative effects of being ordered to create a master key, without having to meet a definition of master key.

As to whether the DOJ is ordering Apple to create a backdoor, given the lack of a precise definition, it is more difficult to answer this question. If one accepts the general concept of what a backdoor means in the computer world and one assumes that the backdoor must be standard for all devices, one must then conclude that Apple is not being ordered to create a backdoor as it will require some level of modification in order for GovtOS/SIF to be installed on other devices.

Because the terms are not defined in their respective documents, it cannot be determined whether Apple is truly required to create a master key (or something equivalent to one), a backdoor, or something two-steps away from a master key or backdoor. However, in future cases, one must closely examine Apple's choice of terms/phrases as well as focus on how much of a modification is required, and its impact to what iPhone models.

E. Is Apple Being Ordered to Hack its Customers?

Initially, in its Message, Apple states, "[t]he government is asking Apple to hack our own users."[130] In its Motion to Compel, the DOJ subsequently denies Apple's public position and argues the Order "does not require Apple to 'hack [its] own users'"[131] nor is it "a 'hack' to all of Apple's encryption software."[132] Then, in Apple's Motion to Vacate and Reply, Apple modifies its public position of hacking its own customers by arguing the Government will have the ability to hack into iPhones once it has the ability to access the iPhone 5C used by one of the attackers through a court order.[133] Apple also additionally argues that the court did not properly analyze *N.Y. Telephone Co.'s* factors to determine whether the AWA could be used to compel third parties (e.g. Apple) to hack into iPhones or whether this hacking would adversely affect its interests.[134]

---

127 Motion to Vacate, *supra* note 18, at 2-3.
128 *See supra* text accompany note 93.
129 Motion to Vacate, *supra* note 18, at 3.
130 Cook, *supra* note 32.
131 Memorandum, *supra* note 70, at 2.
132 Pluhar Supplemental Declaration, *supra* note 12, at 2.
133 Motion to Vacate, *supra* note 18, at 2; s*ee* Reply, *supra* note 42, at 5.
134 Motion to Vacate, *supra* note 18, at 28 (discussing the factors of *N.Y. Telephone Co.'s* like whether the All Writs Act could be used to compel third parties to hack into

In order to answer the question whether the Order requires Apple to hack iPhones or is being ordered to hack its customers, one must again know the definition of the term "hack" and the term "hacker." Similar to the terms "backdoor" and "master key", both parties fail to provide a definition for the term "hack." Rather, they appear to argue their own nefarious understanding of such terms.

Over time the terms "hacker" and "hack," and their meanings have not only changed but have multiplied.[135] According to Jessie Sheidlower, president of the American Dialect Society, the terms early references to machines "share a relatively benign sense of 'working on' a tech problem in a different, presumably more creative way than what's outlined in an instruction manual."[136] It was not until the 1960s that the terms "hack" and "hacker" were incorporated into the vocabulary of computer enthusiasts.[137] *The Jargon File* has eight definitions for the term "hacker," and only one of the definitions (the last definition) has a nefarious/malicious intent, and that definition is "[deprecated] A malicious meddler who tries to discover sensitive information by poking around"[138] Interestingly, the first definition is "A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.'"[139]

Like "hacker," the term "hack" also has multiple definitions that also are not nefarious except for it being an abbreviated term for "hacker."[140] In spite of the mostly benign definitions, over time, most individuals have come to understand the term "hack" to mean malicious meddling. In addition, the use of adjectives are now associated with hackers, e.g., white hat hackers (free-spirited creation), black hat hackers (malicious meddling).[141] However, in spite of the general acceptance of the terms' negative inferences, computer enthusiasts still use the term very differently, at least according to Ben Yagoda of *The New Yorker*. For, "[e]ven as the mainstream usage of 'hacker' took on its darker connotation, the geeks [have] continued using it to mean what it always had: a righteous dude."[142]

In the DOJ–Apple dispute, Apple again focuses on the Government's future,

---

phones, whether the cellphone company was "too far removed" from the matter, or whether hacking into the phone adversely affected the company's interests.).

135 Ben Yagoda, *A Short History of "Hack"*, THE NEW YORKER (Mar. 6, 2014), https://www.newyorker.com/tech/elements/a-short-history-of-hack.

136 *Id.*

137 *Id.*

138 *Id.*

139 *Id*.

140 *See* Hack, THE JARGON FILE, http://catb.org/jargon/html/H/hack.html (last visited Feb. 7, 2018).

141 Yagoda, *supra* note 135.

142 *Id*.

hypothetical actions that would still be subject to judicial review. Next, even if one were to accept the nefarious inference of the term "hack" (or "hacker"), is one really a malicious meddler looking for sensitive information (or even someone creatively exploring the computer's capabilities) when a court has ordered a search, based upon probable cause, and/or the owner of the iPhone has consented to the search as well as to Apple's technical assistance? One would think not. Rather, Apple again appears to use terms without meeting their definitions, and still obtains the benefits of the terms' negative inference.

V. DID THE COURT EXCEED ITS JURISDICTIONAL AUTHORITY WHEN IT ISSUED THE ORDER PURSUANT TO THE ALL WRITS ACT?

Apple argues the Order violates the Constitution as the court exceeded its constitutional authority and violated the separation of powers doctrine when it issued the Order pursuant to the AWA. Apple's jurisdictional arguments include the applicability of the Communications Assistance for Law Enforcement Act[143] ("CALEA")[144] to the issue before the court, Congress' and the Executive Branch's decisions to not pass legislation mandating decryption, and the political question of the issue before the court. Each is an independent basis demonstrating a court's overreach. The DOJ disagrees with Apple's positions and argues the court was within its constitutional authority to issue the Order pursuant to the AWA.

A. The Court's Jurisdiction and Its Relationship to the AWA

Establishing the Judicial Branch, Article III of the Constitution states, "[t]he judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish."[145] The First Congress subsequently established the federal judicial system pursuant to the Judiciary Act of 1789,[146] which also included the original AWA. Today, the AWA states, "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[147] While the statute is straight forward, each party has its own perspective as to the court's jurisdictional authority to issue the Order pursuant to the AWA.

---

143 47 U.S.C. §§ 1001-1010 (2015).
144 Motion to Vacate, *supra* note 18, at 9.
145 U.S. CONST. art. III, § 1.
146 Judiciary Act of 1789, 1 Stat. 73 (1789).
147 28 U.S.C. § 1651(a) (2015).

However, before examining each party's perspective, there are two important principles of the AWA as it relates to a court's jurisdictional authority.

The first fundamental principle of the AWA is that "it neither enlarges nor expands jurisdiction of the court; it may be invoked only to aid jurisdiction which the Court already has."[148] Thus, a court may not use the AWA to extend its authority into areas where it otherwise does not have jurisdiction.[149] A second principle of the AWA is that it "is a residual source of authority [for courts] to issue writs that are not otherwise covered by statute. "Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling."[150] When analyzing the court's authority to issue an AWA order, rather than examining the court's initial jurisdictional authority relied upon (i.e. the search warrant), perhaps it is more efficient to first ask whether there is a statute that specifically addresses the particular issue at hand. Then, if another statute (e.g., CALEA) is controlling, the court's use of the AWA to issue the Order to Apple would not be authorized and no further legal analysis would be required.

B. Is There a Statute that Specifically Addresses the Particular Issue Presented in the DOJ–Apple Dispute?

Apple believes CALEA is a statute that specifically addresses the particular issue at hand because:

> Congress, through CALEA, specified when a company has an obligation to assist the government with decryption of communications, and made clear that a company has no obligation to do so where . . . the company does not retain a copy of the decryption key. Congress . . . opted *not* to provide authority to compel companies like Apple to assist law enforcement with respect to data stored on a smartphone they designed and manufactured.[151]

Not surprisingly, the DOJ's position is CALEA does not "'specifically address'—or even vaguely address—the duty of Apple to assist in extracting data from a passcode-locked cell phone in order to permit the government to execute a validly issued search warrant."[152] Again, polar positions which can be reduced to the following questions: What does CALEA apply to? Data in motion? Data at rest? If only to data in motion, what intercepted communications are to be decrypted?

---

148 U.S. v. Hall, 583 F.Supp. 717, 718 (E.D. Va. 1984).
149 *Id.*
150 PA Bureau of Corr. v. U.S. Marshall Serv., 474 U.S. 34, 43 (1985).
151 Motion to Vacate, *supra* note 18, at 8.
152 Motion to Compel, *supra* note 11, at 22.

The DOJ correctly argues that this case is about data at rest (i.e. stored data) and not the interception of data within a communication. CALEA relies upon definitions in the Wiretap Act,[153] which applies to information acquired during the transmission of a communication and not to stored information, therefore, CALEA is inapplicable.[154] The DOJ emphasizes CALEA requirements that telecommunications carriers retain the capability to comply with court orders for real-time interceptions (data in motion) and outlines what telecommunication carriers must do, in advance of court orders, to ensure their systems can isolate information to allow for the real-time interception of network communications.[155] In this DOJ–Apple dispute, the FBI is not requiring assistance for the decryption of data in motion, but decryption of the device's stored data. Thus, CALEA is inapplicable.

In both its Motion to Vacate and Reply, Apple cites a statute that pertains to the interception of communications (data in motion) yet then concludes that Congress chose not to apply CALEA's requirements to data in storage. However, Apple fails to provide any logical analysis as to how it reaches this conclusion. Apple simply makes general statements similar to the following: "CALEA defines the circumstances under which private companies must create systems to assist law enforcement in its investigatory efforts, as well as the circumstances where such providers are not and cannot be required to build programs and systems to enable law enforcement access."[156] This statement is accurate at least with regards to when private companies are required to assist law enforcement with the interception of communications, data in motion.

Regarding the DOJ's argument of CALEA's applicability to the data in motion versus data at rest, Apple fails to address this argument in either its Motion to Vacate or its Reply. For instance, Apple cites to *In re Order Requiring Apple Inc., to Assist in the Execution of a Search Warrant Issued by This Court* where the Government raised the data in motion versus data at rest argument and lost on that issue.[157] Apple simply references the case as legal support for a court finding the government's use of the AWA to require Apple's decryption assistance was improper.[158]

Although Apple fails to reference this case for a court's rejection of the data at rest argument, the court's reasoning in rejecting the argument must be examined. The court wrote,

> The proposition that CALEA makes a distinction between data 'at rest' and 'in motion' is largely correct as far as it goes, but ultimately

---

153 18 U.S.C. §§ 2510 (2016).
154 *See* Motion to Compel, *supra* note 11, at 22-23.
155 *Opposition*, *supra* note 13, at 12.
156 Reply, *supra* note 42, at 7.
157 *In re* Apple, Inc., 149 F.Supp.3d 341, 355 (E.D.N.Y. 2016).
158 Motion to Vacate, *supra* note 18, at 22.

> misses the point. Even if Congress did not in any way regulate data 'at rest' in CALEA, it plainly could, and did, enact such legislation elsewhere. *See e.g.* 18 U.S.C. § 2703(f)(1) (requiring '[a] provider of wire or electronic communication services or a remote computing service, upon request of a governmental entity, [to] take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court or other process.')[159]

Interestingly, the court's data at rest reference is to the Stored Communication Act[160] ("SCA"), which outlines the responsibilities entities must comply with when preserving stored data. In addition, if the government wishes to access stored data, the SCA generally requires the government to obtain a search warrant.[161] Thus, the court's reasoning appears to be circular as the SCA does not address the issue of encrypted stored data or CALEA. If the SCA requires a search warrant in order to access stored data (assuming all other SCA requirements have been met),[162] the question still remains whether it is permissible to use the AWA to require third party (i.e. Apple's) assistance in accessing the encrypted stored data.

Finally, 18 U.S.C. §§ 2510-2522, the Wire and Electronic Communications Interception and Interception of Oral Communications Act, commonly referred to as the Wiretap Act, provides guidance concerning the enforcement of CALEA. When one examines Section 2522 of the Wiretap Act, Enforcement of the CALEA, it references 18 U.S.C. §§ 2510-2522 (Chapter 119, the Wiretap Act), a State statute, the Foreign Intelligence Surveillance Act of 1978, and 18 U.S.C. §§ 3121-3127 (Chapter 206), use of pen registers or trap and trace devices,[163] i.e., generally statutes pertaining to data in motion. The enforcement provision does not reference the SCA[164] nor does the SCA reference CALEA. Thus, one may conclude that CALEA, with its own enforcement provision, does not implicate or apply to stored data.

When examining Apple and the DOJ's arguments, the DOJ has the stronger argument that CALEA is inapplicable to the Order issued pursuant to the AWA as CALEA applies to the interception of digital (and other) communications (data in motion) and not to stored data (data at rest).

---

159 *In re Apple, Inc.*, 149 F.Supp.3d at 355-56.

160 18 U.S.C. §§ 2701-2712 (2016).

161 *Id.* at § 2703(b)-(d).

162 A discussion on the Stored Communication Act ("*SCA*") could be a separate article. The intent is simply to show how circular the court's logic/argument was with its reference to the *SCA* and the *SCA's* requirement for a search warrant.

163 18 U.S.C. §§ 3121-3127.

164 *See id.* § 2522.

C. The Court's Underlying Authority to Issue the Order Pursuant the AWA

The issue in the DOJ-Apple dispute highlights how the courts utilized the AWA to issue the Order. In the DOJ–Apple dispute, as in *United States v. N.Y. Telephone Co.*,[165] the court's underlying authority was based upon a probable cause search warrant.[166] The DOJ consistently argues this same authority in its *Motion to Compel* and *Opposition*.[167] Other cases where the court's underlying authority to issue a valid AWA order based upon a probable cause search warrant include *Michigan Bell Tel. Co. v. United States*,[168] *In re Application of the United States*,[169] *In re Order XXX, Inc.*,[170] *In re Application of the United States for Order Directing Access to Videotapes*,[171] and *United States v. Hall*.[172] Thus, there is ample case law which supports the court's authority to issue an order requiring third party assistance to effectuate and prevent the frustration of an order it had previously issued and was based upon jurisdiction it otherwise possessed. In other words, issuance of an order allows the government to execute a search warrant.

In past cases where Apple was not a party to the litigation, Apple has responded to AWA orders issued "to facilitate the execution of search warrants on Apple devices running on earlier versions of iOS"[173] which would have been to access unencrypted data in iPhones.[174] Apple also acknowledges compliance with these past orders.[175] This history shows Apple recognized a probable cause search warrant as a court's authority to issue an AWA order. If one has accepted

---

165 United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

166 *Id.* at 168-69.

167 Motion to Compel, *supra* note 11, at 7-10; Opposition, *supra* note 13, at 8, 13.

168 Michigan Bell Tel. Co. v. United States, 565 F.2d 385, 389-90 (6th Cir. 1977) (finding that when the government sought a search warrant for a wiretap based on an FBI agent's information of an illegal gambling business, there was sufficient probable cause).

169 *In re* Application of the United States America for an Order Directing a Provider of Comm. Serv. to Provide Tech. Ass. To Agents of the U.S. Drug Enforcement Admin., 128 F.Supp.3d 478, 484 (D.P.R. 2015) (stating that even though the government had not sought a warrant, there was sufficient probable cause established with an affidavit by a DEA agent).

170 *In re* Order Requiring XXX, Inc., 14 Mag. 2258, 2014 U.S. Dist. LEXIS 154743, at *1 (S.D.N.Y. 2014) (ordering a company to attempt to unlock a cell phone because the government had established probable cause and obtained a search warrant for the phone).

171 *In re* Application of the United States for Order Directing Access to Videotapes, No. 03-89, 2003 U.S. Dist. LEXIS 15227, at *1 (D. Md. Aug. 22, 2003) (finding that the government did not need a court order to review the surveillance footage of an apartment complex because there was no expectation of privacy and the order to force the complex to produce the footage is not burdensome since the agents can review the footage at the complex with the complex's equipment).

172 United States v. Hall, 583 F.Supp. 717, 717 (E.D. Va. 1984).

173 Motion to Compel, *supra* note 11, at 2; Opposition, *supra* note 13, at 6, 28.

174 Motion to Vacate, *supra* note 18, at 2, 28-29; Neuenschwander Declaration, *supra* note 35, at 6.

175 Motion to Vacate, *supra* note 18, at 28-29.

a search warrant as a basis for a court's underlying authority to issue an order against a third party for technical assistance under the AWA, the issue becomes focused as to whether the court exceed its authority under the AWA as a court may not impose unreasonable burdens on Apple.[176]

D. Apple's Other Jurisdictional Arguments

Apple makes a number of other arguments challenging the court's jurisdiction and alleging the court violated the separation of powers doctrine and crossed into legislating. These arguments include expanding *sub rosa* the scope of CALEA obligations to Apple through the Order; updating, repurposing and/or reinventing the statute; and imposing CALEA requirements upon it even when Congress chose not to update CALEA and the Executive Branch chose not to proceed with CALEA II, which would have mandated backdoors for encrypted communications.[177]

Focusing again on CALEA, Apple argues that it does not meet the definition of a telecommunications provider, but rather meets the definition of an information service provider, and Congress excluded information service providers from CALEA's requirements. In addition, CALEA prohibits the government from "dictat[ing] to providers of electronic communications services or manufactures of telecommunications equipment any specific equipment design or software configuration."[178] And, even if Apple was a covered telecommunication provider, which Apple does not concede, CALEA "does not require covered telecommunication carriers . . . to be responsible for 'decrypting, or *ensuring the government's ability to decrypt*, any communication."[179] Whether Apple meets the definitions under CALEA is immaterial because CALEA is inapplicable to the specific issue of third party assistance for accessing stored, encrypted data. The Order was issued in accordance with the AWA based upon the underlying court's authority to issue a probable cause search warrant and not pursuant to CALEA. As such, the focus of the Order's validity and whether the court exceeded its authority should be based upon *N.Y. Telephone Co.'s* three-prong analysis.[180]

Apple also argues the court exceeded its authority, and improperly crossed into the role of legislating by repurposing and reinventing CALEA to meet the evolving needs of society. Apple further argues, only Congress "has authority

---

176 *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 172-73 (1977).
177 *See* Motion to Vacate, *supra* note 18, at 8-9, 18.
178 *Id.* at 16.
179 *Id.* at 17.
180 *N.Y. Tel. Co.*, 434 U.S. at 174-75.

'to update' a 'technologically antiquated' statute 'to address the new and rapidly evolving era of computer and cloud-stored, processed and produced data.'"[181] Like Apple's CALEA definitions' argument, Apple's repurposing and reinventing a statute argument is simply misplaced. The AWA authorizes a court to "'avail itself of all auxiliary writs as aids in the performance of its duties, when the use of such historic aids is calculated in its sound judgment to achieve the ends of justice entrusted to it.' The Court has consistently applied the Act flexibility in conformity with these principles."[182] Thus, Congress has given the courts a source of procedural authority to issue auxiliary writs in order to achieve justice or to prevent the circumvention of justice. The underlying court's authority in the DOJ–Apple dispute was not CALEA; it was the probable cause search warrant. The court was not attempting to update CALEA, and Apple's insertion of CALEA in this argument simply confuses the issue. If the court exceeded its authority, it would be based upon *N.Y. Telephone Co.'s* three-prong analysis,[183] and not because it was attempting to update a statute that it did not rely upon to issue its order.

Apple also argues the court lacks judicial authority as the Executive Branch abandoned CALEA II which would have mandated backdoors of encrypted communications.[184] In addition, the combination of Congress leaving CALEA untouched[185] with three recent legislative proposals, which would have affirmatively prohibited the government from forcing companies to compromise data security,[186] indicate Congress has not yet made a decision "to act on this issue."[187] Both Apple and the DOJ cite *Central Bank of Denver v. First Interstates Bank of Denver*, ("*Central Bank*")[188] albeit for different purposes. The DOJ relies upon *Central Bank* as legal authority of the Court's reluctance to rely upon failed legislative proposals to demonstrate Congress' intent.[189] The Court wrote, "failed legislative proposals are 'a particularly dangerous ground on which to rest an interpretation of a prior statute. Congressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction, including the inference that the existing legislation already incorporated the offered change.'"[190] In reviewing *Central Bank*, it is

---

181 Motion to Vacate, *supra* note 18, at 18.
182 *N.Y. Tel. Co.*, 434 U.S. at 173.
183 *Id.* at 174-78.
184 *See* Motion to Vacate, *supra* note 18, at 18-19.
185 *See id.* at 6, 8-9, 18-19.
186 *Id.* at 9.
187 *Id.* at 9 n.16.
188 Central Bank of Denver v. First Interstate Bank of Denver, 511 U.S. 164 (1994), *superseded in part by statute*, Private Securities Litigation Reform Act of 1995, Pub. L. No. 104-67 (1995).
189 Motion to Compel, *supra* note 11, at 24; Opposition, *supra* note 13, at 8.
190 *Central Bank of Denver*, 511 U.S. 164, 187 (1994).

important to consider the Court's acknowledgement that its cases have not been entirely consistent on legislative inaction and intent. However, after acknowledging this inconsistency, the Court reiterated its position that the absence of corrective legislation "arguments deserve little weight in the interpretive process"[191] as "'[w]e walk on quicksand when we try to find in the absence of corrective legislation a controlling legal principle.'"[192] Apple concedes "silence is sometimes a weak indicator of intent;"[193] however, congressional inaction can be an indicator of intent "when Congress actively considers legislation to address a major policy issue, yet deliberately declines to enact it"[194] or when congressional inaction occurs within "the context of an elaborate and comprehensive statutory scheme."[195]

Apple emphasizes "Congress has intentionally opted not to compel third parties' assistance in retrieving stored information on devices. That Congress, confronted . . . with the contentious debate . . . among competing security and privacy interests, made this decision, [which] 'indicates a deliberate congressional choice with which the court should not interfere.'"[196] Apple's argument is misplaced as it again relies upon CALEA and the requirements defined entities have regarding the interception of encrypted communications to conclude that "Congress has intentionally opted not to compel third parties' assistance in retrieving"[197] encrypted stored data. While Apple's reliance of a comprehensive regulatory scheme may be applicable to the interception of encrypted communications, the Wiretap Act[198] and CALEA; it does not follow that it applies to stored, encrypted data. Finally, Apple cites *Bob Jones University v. United States*,[199] as legal authority to demonstrate congressional intent based upon congressional inaction. However, in *Bob Jones University*, the Court was examining the inference of congressional inaction as to whether Congress agreed with *past* published IRS opinions. In this case, there is no evidence to buttress an inference that Congress' lack of action is in support of past court opinions concerning the use of AWA to require Apple's technical assistance to aid the FBI in accessing stored, encrypted data.

Apple's final jurisdictional argument is whether "Apple should be compelled to create a back door to their own operating systems to assist law enforcement

---

191 *Id*.
192 *Id.* at 186 (citing Helvering v. Hallock, 309 U.S. 106 (1940)).
193 Reply, *supra* note 42, at 11.
194 *Id*.
195 *Id*.
196 Motion to Vacate, *supra* note 18, at 18.
197 *Id*.
198 18 U.S.C. §§ 2510-2522 (2012).
199 Bob Jones Univ. v. United States, 461 U.S. 574, 596 (1983).

is a political question, not a legal one."[200] Both parties cite *Baker v. Carr*[201] and *Diamond v. Chakrabarty*[202] to support and refute each other's political question jurisdictional argument. Thus, one must ask when is an issue a political question and outside a court's jurisdiction?

In *Vieth v. Jubelirer*, the Court provided the following six independent tests for answering this question:

> (1) [A] textually demonstrable constitutional commitment of the issue to a coordinate political department; or (2) a lack of judicially discoverable and manageable standards for resolving it; or (3) the impossibility of deciding without an initial policy determination of a kind clearly for nonjudicial discretion; or (4) the impossibility of a court's undertaking independent resolution without expressing lack of the respect due coordinate branches of the government; or (5) an unusual need for unquestioning adherence to a political decision already made; or (6) the potentiality of embarrassment from multifarious pronouncements by various department on one question.[203]

Although the *Vieth* Court stated "[t]hese tests are probably listed in descending order of both importance and certainty,"[204] the *Baker* Court stated 'the appropriateness under our system of government of attributing finality to the action of the political departments and also the lack of satisfactory criteria for a judicial determination are dominate considerations"[205] for determining the existence of a political question.[206] Thus, the DOJ's statement that the political question doctrine, "applies not in every case raising policy considerations but only in cases that raise nothing *but* policy considerations, cases where there is a 'lack of judicially discoverable and manageable standards for resolving' the issue"[207] finds support with *Baker (*as well as both *Diamond* and *Zivotosky v. Clinton*[208]).

Apple's arguments are misplaced regarding the lack of finality of action by political departments and that an initial policy decision has not been made. The Supreme Court had held that a search warrant is required to search a

---

200 Motion to Vacate, *supra* note 18, at 19.

201 Baker v. Carr, 369 U.S. 186, 217 (1962) (holding that a case is a political question if it requires "an initial policy determination of a kind clearly for nonjudicial discretion").

202 Diamond v. Chakrabarty, 447 U.S. 303, 317 (1980) (holding that courts cannot make choices on "a matter of high policy for resolution within the legislative process after the kind of investigation, examination, and study that legislative bodies can provide.").

203 Vieth v. Jubelirer, 541 U.S. 267, 277-78 (2004) (citing *Baker*, 369 U.S. at 217).

204 *Id.* at 278.

205 *Baker*, 369 U.S. at 210 (citing Coleman v. Miller, 307 U.S. 433, 454-55 (1939)).

206 *Id*.

207 Opposition, *supra* note 13, at 7-8.

208 Zivotofsky v. Clinton, 566 U.S. 189, 207 (2012).

smartphone.[209] Accordingly, the AWA authorizes the use of a writ to require assistance from a third party to ensure the search warrant can be properly executed. The issue before the court is not a political question but whether the court appropriately used the AWA to issue the required technical assistance as articulated in *N.Y. Telephone Co.*[210]

VI. DID THE COURT APPROPRIATELY USE THE AWA WHEN IT ORDERED APPLE TO PROVIDE THE MANDATED TECHNICAL ASSISTANCE?

Case law has been recognized and accepted that courts may utilize the AWA "to provide [courts] the instruments necessary to perform their duty, assuming those instruments are 'agreeable' to the usages and principles of law."[211] In examining both parties court-filed documents, each party agrees that a court may utilize the AWA to require assistance from a third party not subject to the litigation, and a probable cause search warrant could be the court's underlying authority to issue the order. The parties differ on whether it was appropriate for the court to issue this Order via the AWA, requiring the described technical assistance from Apple.

The DOJ argues the court properly utilized the AWA and all necessary requirements under the AWA have been met. Apple disagrees, arguing all necessary requirements under the AWA have not been met. In examining whether the use of the AWA was agreeable to the usages and principles of law, one must turn to *N.Y. Telephone Co*., the case which is "the acme of such litigation and the standard by which such procedures are now judged"[212] In *N.Y. Telephone Co.,* the Court concluded a court has the authority to use the AWA to require assistance from one non-party to the litigation; however, the Court also recognized a court's authority is limited as it may not impose unreasonable burdens upon the third party.[213] The Court outlined a three-prong test for future courts to consider when determining whether an order is reasonable. Applying *N.Y. Telephone Co.'s* three-prong test to Apple, the issues are the following: "(1) How far removed is Apple from the underlying controversy? (2) How burdensome or unreasonable is the Order? (3) How necessary is Apple's assistance?"[214]

---

209 Riley v. California, 134 S. Ct. 2473, 2495 (2014).
210 United States v. N.Y. Tel. Co., 434 U.S. 159, 176 (1977).
211 United States v. Li, 55 F.3d 325, 329 (7th Cir. 1995).
212 United States v. Hall, 583 F.Supp. 717, 718 (E.D. Va. 1984) (citing United States v. N.Y. Tel. Co., 434 U.S. 159 (1977)).
213 *N.Y. Tel. Co*., 434 U.S. at 172.
214 *See id.* at 172-76.

Unfortunately, the *N.Y. Telephone Co.* Court combined the articulated factors with the facts of the case (as opposed to establishing elements to consider) to conclude the order was within the lower court's authority. Apple is correct that the government fails to cite one case directly on point to the required assistance described in this particular *Order*;[215] however, this fact alone is not dispositive. The fact that a court has been presented a request for technical assistance that has never been previously addressed does not prevent the court from deciding whether the use of the AWA was appropriate. This was seen in *United States v. Hall* where the district court had to determine whether it was appropriate to issue an order, pursuant to the AWA, requiring a bank to produce the credit card records of the girlfriend of a fugitive.[216] At that time, the closest parallel cases pertained to the installation of telephone pen registers.[217] Despite the existence of a case with analogous facts, the *Hall* court still concluded that all AWA requirements had been met, and it had the authority to issue the AWA order requiring the bank to provide the credit card records.

In challenging the court's Order, Apple argues it gives the Government unlimited power, stating, "what is to stop the government from demanding that Apple write code to turn on the microphone in aid of government surveillance, activate the video camera, surreptitiously record conversations, or turn on location services to track the phone's user? Nothing."[218] Apple adds the DOJ's interpretation of the AWA is unlimited, with no boundaries,[219] and its interpretation would permit it

> to force citizens to do all manner of things 'necessary' to assist it in enforcing the laws, like compelling a pharmaceutical company against its will to produce drugs needed to carry out a lethal injection in furtherance of a lawfully issued death warrant, or requiring a journalist to plant a false story in order to help lure out a fugitive, or forcing a software company to insert malicious code in its auto-update process that makes it easier for the government to conduct court-ordered surveillance.[220]

The DOJ correctly notes that Apple is providing hypotheticals, and courts do not address hypotheticals; they address concrete disputes.[221] In addition, all future requests for assistance via the AWA would be subject to a court's review, and third parties would be given an opportunity to object to the court's authority as

---

215 Motion to Vacate, supra note 18, at 1, 30.
216 United States v. Hall, 583 F.Supp. 717, 717-18 (E.D. Va. 1984)
217 *Id*. at 718.
218 Motion to Vacate, *supra* note 18, at 4.
219 *See* Reply, *supra* note 42.
220 Motion to Vacate, *supra* note 18, at 26.
221 *See* Clapper v. Amnesty Int'l, 568 U.S. 398, 408-10 (2013); *see also infra* notes 358-373 with accompanying text.

was done in this case and in the cases cited. The future hypothetical cases would need to cite the court's underlying jurisdictional authority (e.g. Federal Rules of Criminal Procedure, Rule 41) in order to avail itself of the AWA, and demonstrate how *N.Y. Telephone Co.'s* three-prong test has been met. As to Apple's hypotheticals, if they do occur, they will be resolved in court at the time those facts present themselves.

A. How Far Removed Is Apple From the Underlying Controversy?

Under the three-prong test, if Apple is too far removed from the underlying controversy, then the court has exceeded its authority to issue the Order pursuant to the AWA.[222] Unfortunately, *N.Y. Telephone Co.* did not provide specific elements to consider when analyzing whether a third party is too far removed from the controversy. The Court simply explained why the telephone company was not too far removed. Specifically,

> [T]here was probable cause to believe that the Company's facilities were being employed to facilitate a criminal enterprise on a continuing basis. For the Company, with this knowledge, to refuse to supply the meager assistance required by the FBI in its efforts to put an end to this venture threatened obstruction of an investigation which would determine whether the Company's facilities were being lawfully used. Moreover, it can hardly be contended that the Company, a highly regulated public utility with a duty to serve the public, had a substantial interest in not providing assistance.[223]

The DOJ provides several, varied reasons demonstrating how Apple is not too far removed, while Apple provides a list of reasons as to why it is too far removed from the controversy. In examining the DOJ's argument, one must remember there was probable cause to believe the device contained encrypted data related to the underlying terrorist event.[224] In its motions, the DOJ focuses on the close relationship between Apple and its iPhones. The DOJ argued that:

> (1) Apple designed, manufactured and sold the device;
> (2) Apple is the creator and owner of the software operating system, marketed under the name "iOS," within the device;
> (3) Apple designed the encryption and non-encryption features within the device;
> (4) Apple designed the device such that only Apple signed software can run on the device and its operating system which prevents the FBI from using another type of software on the device (to recover

---

222 *See* Order, *supra* note 27, at 1-2.
223 United States v. N.Y. Tel. Co., 434 U.S. 159, 174 (1977).
224 Motion to Compel, *supra* note 11, at 19.

data or test passcodes);
(5) Apple does not sell its operating system but only licenses it and the licensing agreement prohibits the user from transferring any ownership of the operating system;
(6) Apple restricts access to its software source code;
(7) Only Apple can update the device;
(8) Apple has the ability with older operating systems to obtain the unencrypted file content from iPhones without the passcode, and routinely did so when a search warrant accompanied an AWA Order;
(9) Apple has the ability to modify the software to accomplish what the FBI has requested and what the court has ordered;
(10) Apple has the technical capability to assist the government given the encryption and security features were designed by Apple, implemented by Apple, and routinely updated by Apple through its cryptographic signature of iOS patches and updates;
(11) Apple has not denied it has the technical capability to assist the Government; and
(12) Only Apple can provide the assistance.[225]

Thus, when one considers all these factors identified by the DOJ, Apple is not far removed from the controversy.

Strongly disagreeing with the DOJ and arguing it was too far removed from the controversy, Apple focuses on distinguishing itself from *N.Y. Telephone Co.* More specifically,

(1) Apple is a private company;
(2) Apple does not own the device;
(3) Apple has no connection to the encrypted data contained within the device;
(4) Apple has no connection to the events leading up to the investigation, versus *N.Y. Telephone Co.* where the company's phone lines were being used to commit a crime;
(5) Apple is not a highly regulated telecommunication agency with a duty to serve the public;
(6) Apply is not a monopoly essential to communications;
(7) Apple is a private company that believes encryption is crucial to protecting the security and privacy of its devices;
(8) Apple's encryption and non-encryption security features are recommended industry standards which are followed not only by Apple, but by other private companies;
(9) Even though Apple designed, manufactured and sold the device as well as wrote and owns the software and iOS, this is insufficient to establish the connection mandated by *N.Y. Telephone Co.* for the AWA does not allow the government to compel a manufacture

---

[225] *Id*. at 17.

> simply because a commercial item is introduced into commerce;[226] and "Apple is no more connected to this phone than General Motors is to a company car used by a fraudster on his daily commute."[227]

Although Apple argues it is not a highly regulated utility company with a duty to serve the public, AWA cases are not limited to regulated public utility entities; private companies have also been ordered to provide assistance to the Government. For instance, in *United States v. Hall,* an order against a bank for bank records was issued,[228] and *In re Application of U.S. for an Order Directing X to Provide Access to Videotapes* there was an order against an apartment complex to provide the government its videotapes.[229] The AWA cases requiring assistance from private or public companies recognized those entities' duty to the public because they were "in a position to frustrate the implementation of a court order or the proper administration of justice."[230] Similarly, Apple's "refusal to help law enforcement efforts, when it has the ability to do so, could materially"[231] frustrate the court order (i.e. search warrant) and the proper administration of justice.

While Apple is not a public utility monopoly in the traditional sense, Apple has monopolistic characteristics similar to public utilities, given its level of control over its products, especially after it has sold the product. Apple compares itself to General Motor's ("GM") distance from a GM automobile used by a criminal in his daily commute, with GM being too far removed from any crime.[232] However, Apple's argument is misplaced. With a probable cause search warrant, the FBI can place a tracker on the automobile or can search the automobile, and the FBI does not need a need a GM mechanic to assist with the placement of the tracker or with the search of the car. Furthermore, non-GM parts can be used on a GM automobile and non-GM mechanics may work on the automobile. Finally, Apple's arguments that the DOJ's licensing argument "is a total red herring" and "[a] licensing agreement no more connects Apple to the underlying events than a sale"[233] are also misplaced as the licensing agreement prohibits anyone from selling the software to a third party, e.g. the FBI, where it could potentially circumvent iOS. Thus, Apple has limited the Government's options, thereby creating a monopoly around its devices and its iOS.

---

226 Motion to Vacate, *supra* note 18, at 22.
227 *Id.*
228 United States v. Hall, 583 F.Supp. 717, 722 (E.D. Va. 1984).
229 *In re* United States For Order Directing Access To Videotapes, No. 03-89, 2003 U.S. Dist. LEXIS 15227 at *1 (D. Md. Aug. 22, 2003).
230 *Hall*, 583 F. Supp. at 720-21.
231 *Id*. at 721.
232 Motion to Vacate, *supra* note 18, at 22.
233 *Id.*

In both its Motion to Vacate and Reply, Apple argued any criminal activity linked to the device at issue ended over two months ago when the terrorist was killed.[234] While the court proceeding was more than two months later, that in and of itself is not dispositive. The FBI had probable cause to believe the device contained information about the terrorist attack.[235] The encrypted data may have the contacts and resources used in the December 2015 attack and potential future attacks. The government should explore how the attack occurred in order to prevent future attacks, including identifying the steps followed and determining what steps could be implemented to prevent future attacks. Finally, some courts have decided AWA cases after the issue of the authorized use of the AWA had become moot as the AWA legal controversy was repetitive, but its resolution evaded judicial review.[236] Apple's argument that the date the terrorist was killed demonstrates that they are too removed from the controversy is misplaced. It is misplaced because at the time of Apple's March 15, 2016 Reply, the device still contained the encrypted data, the FBI had probable cause to believe the device contained data relevant to the attack, the FBI still needed to examine the device, and the FBI was unable to access the encrypted data because of Apple's security features.

Given both party's arguments, the DOJ has the stronger argument that Apple is not too far removed from the controversy, and the first prong of *N.Y. Telephone Co*. has been met. However, there are two other prongs which must be evaluated before one can conclude the court was authorized to use the AWA to order Apple to provide the technical assistance specified in the Order.

B. Is the Order Requiring Apple's Technical Assistance Burdensome or Unreasonable?

If the Order is too burdensome or unreasonable for Apple, then the second prong, as articulated in *N.Y. Telephone Co.* is not met, and the court would have exceeded its authority under the AWA. Again, *N.Y. Telephone Co.* did not provide specific elements to consider when analyzing whether an order is unreasonable or burdensome for a third party. In *N.Y. Telephone Co.*, the Court simply explained why the order was not burdensome or unreasonable as the order directed the telephone company be reimbursed at prevailing rates and the order required minimal effort from the telephone company.[237] In *United States*

---

234 Reply, supra note 42; Motion to Vacate, *supra* note 18, at 21.

235 *See* Motion to Compel, *supra* note 11, at 1, 5-6; *see also* Opposition, *supra* note 13, at 2, 13.

236 *See* Mich. Bell Tel. Co. v. United States, 565 F.2d 385, 387 (6th Cir. 1977); *In re* United States ex. Rel. an Order Authorizing Disclosure of Location Info. Of a Specified Wireless Tel., 849 F.Supp.2d 526, 532 (D. Md. 2011).

237 United States v. N.Y. Tel. Co., 434 U.S. 159, 175 (1977).

v. Hall, the District Court, modified this prong providing "the order must not adversely affect the basic interests of the third party or impose an undue burden."[238] Apple emphasizes *Hall* to support its argument that the *Order* is contrary to Apple's business interests in protecting the security and privacy of its products.[239]

There are cases which limit a court's use of the AWA where the non-litigant entity bore non-reimbursable costs. One such case is *PA Bureau of Correction v. U.S. Marshall Service*, where the Court stated the AWA "does not authorize them [the courts] to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate,"[240] a statement Apple emphasizes.[241] However, it is clear in *PA Bureau of Correction*, the State was attempting to transfer state prisoner transportation costs (so that prisoners could participate in federal litigation) to the federal government as "the 'deluge of . . . civil rights actions' calls for 'creative' use of federal judicial power to alleviate the drain on the States' fiscs [finances] from the transport of inmates to and from federal courthouses."[242] While the Court concluded the use of the AWA was inappropriate under the particular facts of creative thinking to transfer costs, the Court also left open the door to the future possibility of the use of the AWA to transport state prisoners in cases involving serious security risks as these exceptional circumstances may permit the use of the AWA.[243]

Another case where the use of the AWA is limited because of costs borne by a company is *Plum Creek Lumber Co. v. Hutton*,[244] where the court states the AWA "does not give the district court a roving commission to order a party subject to an investigation to accept additional risks"[245] This is another statement Apple also emphasizes.[246] *Plum Creek Lumber Co.* is a case where OSHA was attempting to use the AWA to require a company to require its employees to wear special hats so that OSHA could conduct a non-criminal investigation. The hats impeded the employees which could have led to personal injuries and the costs of those injuries would have been fully borne by the company. While *Plum Creek Lumbar Co.* and *PA Bureau of Correction* limited the use of the AWA, the underlying cases are civil cases, with the transfer of costs to the employer or a third party. The DOJ correctly identifies criminal investigation cases where

---

238 United States v. Hall, 583 F. Supp. 717, 719 (E.D. Va. 1984).
239 Motion to Vacate, *supra* note 18, at 23.
240 PA Bureau of Corr. v. U.S. Marshal Serv., 474 U.S. 34, 43 (1985).
241 Motion to Vacate, *supra* note 18, at 15; Reply, *supra* note 42, at 4.
242 *PA Bureau of Corr.*, 474 U.S. at 40.
243 *Id*. at 43.
244 Plum Creek Lumber Co. v. Hutton, 608 F.2d 1283, 1289 (9th Cir. 1979).
245 *Id*. at 1289.
246 Motion to Vacate, *supra* note 18, at 1, 15, 31.

courts have found the use of the AWA appropriate to require assistance from those not subject to a litigation so that a court's jurisdiction would not be thwarted. The difficulty, as Apple correctly points out, is that none of these cases are directly on point to the facts of this particular DOJ–Apple dispute, although as previously discussed, this alone is not a dispositive determination.

As to the reasonableness of the Order, the DOJ argues Apple is only required to assist the FBI and this assistance is not unreasonable as it is not a threat to its other products.[247] Additionally, Apple writes code, whether it is new or a modification to its iOS, indicating writing code is not unreasonable or burdensome.[248] Furthermore, Apple does not deny, but rather, concedes it has the technical ability to assist the FBI;[249] and Apple does not argue its assistance would be too labor-intensive or time-intensive, rather it is concerned about the impact to its reputation and marketing strategy which are not direct costs.[250]

In Apple's Motion to Vacate, Apple addresses some of the DOJ's arguments. However, it focuses on the creation of the new operating system adversely affecting its basic interests as a company. More specifically, GovtOS/SIF currently does not exist, Apple has no interest in creating it and would never create it as this new version of the iOS would be designed to defeat critical security features and would require significant resources from Apple as it will need to not only write new code, but disable existing code.[251] Although hard to quantify, the expected expended resources include the following:

> (1) Six to ten engineers working full-time for two to four weeks;
> (2) Costs associated with the design, development and underlying documentation of the tool (GovtOS/SIF);
> (3) Costs associated with the development of detailed documentation instructing the FBI how to use GovtOS/SIF as well any tool used or developed by the FBI to interface with GovtOS/SIF thus allowing the FBI to input the passcodes electronically;
> (4) If GovtOS/SIF is not used in a secure Apple facility, Apple would need to develop procedures to encrypt, validate and input into the device communications from the FBI, and this process would need to be logged in and recorded in the event Apple's methodology is ever questioned or challenged in court;
> (5) Once created, GovtOS/SIF would need to be evaluated through Apple's quality assurance and security testing process. Based upon experiences, problems are expected to occur, therefore the testing process would repeat;

---

247 Motion to Compel, *supra* note 11, at 13-16.
248 *Id*, at 13.
249 *Id.* at 6, 14.
250 *Id.* at 3.
251 Motion to Vacate, *supra* note 18, at 2, 7, 23.

> (6) If GovtOS/SIF is destroyed (or erased/deleted) after employed on the device, GovtOS/SIF would need to be recreated for each new request which will multiply the burden placed upon Apple as other law enforcement agencies are desiring the same assistance, and costs are multiplied; and
> (7) Even if Apple did not destroy GovtOS/SIF, there would security costs associated with protecting GovtOS/SIF as it would be extremely desirable to criminals, terrorists and hackers.[252]

Apple also attempts to distinguish itself from the cases relied upon by the DOJ, arguing it is not tasked to provide "meager assistance"[253] and the cases cited by the DOJ deal with third party records which already exit, such as bank records[254] or videotapes.[255] Apple emphasizes the Order requires it to create entirely new intellectual property it believes is too dangerous to create, and this is vastly different from the cases the DOJ relies upon.[256] Finally, Apple argues the public will bear the burden of the loss of security and privacy of its devices while criminals and terrorists will take advantage of other encrypted protocols.[257]

In its Opposition, the DOJ provides substantial financial information about Apple, relying on Apple's annual report and Apple's status as a Fortune 500 corporation. For example, Apple employs more than 100,000 full-time-equivalent employees;[258] its 2015 annual income was over 200 billion dollars, which is more than the state of California's budget; and its revenues exceed the nominal Gross Domestic Product of two-thirds of the world's nations.[259] One should also consider that Apple has become the *first trillion dollar* company,[260] with $243.7 billion cash on hand, the most of any Fortune 500 company.[261] Another way of trying to comprehend its value, as the first trillion dollar company, Apple has the combined net worth of 21 members of Forbes 2017 list of billionaires.[262]

---

252 *Id*. at 12-14, 24-25.
253 *Id*. at 20.
254 *Id*. at 27-28.
255 *Id*. at 21.
256 *Id*. at 2, 21, 29.
257 *See* Motion to Vacate, *supra* note 18, at 23.
258 Opposition, *supra* note 13, at 21.
259 *Id*.
260 Jack Nicas, *Apple Is Worth $1,000,000,000,000. Two Decades Ago, It Was Almost Bankrupt*, N.Y. TIMES (Aug. 2, 2018), https://www.nytimes.com/2018/08/02/technology/apple-stock-1-trillion-market-cap.html.
261 Victoria Rooney, *Steve Jobs and Apple's prolonged history in seven fast facts*, FOX BUS. NEWS (Aug. 2, 2018), https://www.foxbusiness.com/technology/steve-jobs-and-apples-prolonged-history-in-seven-fast-facts.
262 Nicas, *supra* note 261; Rooney, *supra* note 262.

In addition to considering Apple's financial status, Apple is not fully responsible for the costs of the technical assistance, as Magistrate Judge Pym's Order directed Apple to "advise the government of the reasonable cost of providing this service."[263] The DOJ also acknowledged the Government's obligation to pay reasonable costs for Apple's technical assistance.[264] Thus, if the Government pays for reasonable costs associated with Apple's technical assistance, a portion of Apple's unreasonable and burdensome arguments are negated, which is perhaps one reason why Apple fails to comment on the reimbursement requirement in either its *Motion to Vacate* or *Reply*. Finally, future orders (although hypotheticals which should not be considered by the court) would be compensated in those future cases.[265] As to costs associated with compliance and supplemental procedures, Apple has a centralized process dedicated to compliance with subpoenas[266] and one would conclude Apple would have had to develop protocols for pre-iOS8 systems. While the protocols and procedures may need to be expanded, it is unknown how much the cost difference would be.

In its Reply, Apple again focuses its argument on its position that it would never write the code for the functions required in the Order and that it finds it offensive to build GovtOS/SIF,[267] as compared to *N.Y. Telephone Co*. which routinely used pen registers to detect fraud.[268] The offensiveness aspect of creating GovtOS/SIF is not relevant to a reasonableness analysis given the subjective nature of the term. One could find hundreds of individuals/entities who find certain Government requests or actions offensive. That does not make the Government's actions unauthorized. In addition, some may find Apple's actions offensive as they are protecting the terrorist's data over protecting national security, or so one could argue. Rather than focusing on offensive feelings, Apple should objectively articulate how the Order is a burden or is unreasonable for Apple. More specifically, what the impact to Apple's products is, and whether Apple is being ordered to create a backdoor and/or a master key (or equivalent to a master key).[269] This question could not be conclusively answered because it was unknown to what extent GovtOS/SIF code would need to be modified to work on other iPhones, be it the same iPhone model (e.g. 5Cs or 5s) or all iPhone models. Therefore, it is unknown whether this prong has been met, and the Declarations/testimony from each party will need to address

---

263 Order, *supra* note 27, at 3.

264 Opposition, *supra* note 13, at 21.

265 *Id.* at 21; Nicas, *supra* note 261.

266 *Legal Process Guidelines*, APPLE INC., https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (last visited Mar. 28, 2019).

267 Reply, *supra* note 42, at 17.

268 United States v. N.Y. Tel. Co., 434 U.S. 159, 174-75 (1977).

269 *See supra* text accompany notes 85-122; Zetter, *supra* note 90.

this particular point in future cases.

C. How Necessary Is Apple's Technical Assistance?

N.Y. Telephone Co.'s third prong concerns how necessary was the telephone company's assistance to the investigation.[270] In *N.Y. Telephone Co.*, the FBI could not install the pen registers without tipping off the targets to the investigation. The Court provides little guidance as to how this prong is or is not met as the Court simply wrote "the Court of Appeals recognized, that without the Company's assistance there [wa]s no conceivable way in which the surveillance authorized by the District Court could have been successfully accomplished."[271] There was no further explanation as to what additional steps the FBI was required to take.

The DOJ's position is Apple's assistance is "necessary to effectuate the warrant"[272] in order to search a device critical to an ongoing terrorism investigation as the FBI has reason to believe the device contains critical communications prior to and around the time of the killings. The Device may also contain data that has not yet been accessed through other methods as certain data resides only on the iPhone.[273] Whether there are other methods available to the FBI, "both Apple and the FBI agreed that they were unable to identify any other methods – besides that which is now ordered by this Court – that are feasible for gaining access to the currently inaccessible data"[274] Thus, Apple's technical assistance is consistent with *N.Y. Telephone Co.'s* necessary requirement.

Apple's position is the DOJ must have absolutely no other possibility of accessing the encrypted data, and it must first exhaust all other possible avenues including seeking "technical assistance from other federal agencies with expertise in digital forensics"[275] before receiving Apple's assistance. Apple also argues the FBI prevented access to the encrypted data when it, without contacting Apple, changed the iCloud password associated with the terrorist's account which then prevented the device from initiating an automatic iCloud backup; and had the FBI consulted with Apple before this change, it "could have obviated the need to unlock the phone and thus for the extraordinary order the government now seeks. Had the FBI consulted Apple first, this litigation may

---

270 *N.Y. Tel. Co.*, 434 U.S. at 175.
271 *Id*.
272 Memorandum, supra note 70, at 16.
273 *Id*. at 6.
274 *Id*. at 17.
275 Motion to Vacate, *supra* note 18, at 30.

not have been necessary."[276] In effect, Apple argues the FBI created this situation. Thus, the DOJ has not demonstrated that Apple's assistance was absolutely necessary to effectuating the warrant.

In its Opposition, the DOJ focuses on the structure and security of Apple's iOS as to how and why Apple's assistance is necessary. The DOJ stresses the following:

> (1) Only Apple signed software can be loaded on the device.
> (2) Apple doubts the Government could disable the security features as it has "'insufficient knowledge of Apple's software and design protocols to be effective.'" [277]
> (3) The device was found powered off, and subsequent testing revealed that once powered off, an iPhone will not back itself up to an iCloud account unless and until it has been unlocked with the passcode at least once.
> (4) Evidence suggests that the terrorist had changed his iCloud password on October 22, 2015 (shortly after the last backup of October 19, 2015) and that the auto-backup feature was disabled. Therefore, a forced backup of the device was never going to be successful.
> (5) The iCloud access is not a sufficient substitute for the search of the device as certain information (e.g. keyboard caches/recent keystrokes) is not backed up to the iCloud and resides only within the device.
> (6) Apple's argument that *N.Y. Telephone Co.* requires "absolute necessity" is misplaced as *N.Y. Telephone Co.* rests on the language within the AWA statute itself which is "necessary or appropriate.[278]

In its Reply, Apple argues the FBI should have consulted with other federal agencies before requiring Apple to assist with the investigation, and the FBI created this dilemma of inaccessibility to the encrypted data when the FBI changed the iCloud password. Thus, the DOJ has not met the "no conceivable way" language of *N.Y. Telephone Co.*[279] In order to properly analyze the third prong, one must examine Apple's argument that the FBI created this situation when it changed the iCloud account password.[280] Like other aspects of this case, each party's view of the iCloud account password change is different.

---

[276] *Id*. at 11.
[277] Opposition, *supra* note 13, at 28.
[278] *Id.* at 29-30; *see also* Pluhar Supplemental Declaration, *supra* note 12, at 3-4.
[279] Reply, *supra* note 42, at 22.
[280] Password and passcode are two distinct terms. The passcode is a component of the encryption key that protects the device itself. A password pertains to an Apple ID needed to access Apple's Internet Services, such as iCloud. Each iCloud account is associated with a specific Apple ID. The password necessary to access the iCloud is unrelated to the passcode needed for physical access to the device itself. *See iOS9.0 Security Guide*, *supra* note 45, at 7, 12, 38, 50; *see also* Pluhar Supplemental Declaration, *supra* note 12, at 3.

In its Motion to Compel, the DOJ initially stated the SBCDPH changed the iCloud account password in order to access the iCloud account, as neither the FBI nor SBCDPH knew the iCloud account password. However, in SSA Pluhar's Supplemental Declaration, SBCDPH changed the iCloud account password under his direction.[281] While the change of the password had the effect of eliminating the possibility of an auto-backup, the change of the iCloud password account is immaterial. According to the DOJ, the device was found powered off, and the device's passcode needed to be entered at least once before an auto-backup to the iCloud account would occur. And, because no one knew the passcode, an auto-backup to the iCloud was never going to occur.[282]

In its Motion to Vacate, Apple attacks the FBI's credibility arguing the FBI initially blamed the SBCDPH, then in a press release corrected itself in "that it 'worked with' the County [SBCDPH] to reset the password."[283] Apple then argues the FBI created this situation when it changed the password without checking with Apple or reading its security guide, and by changing the iCloud password, it foreclosed the possibility of the iPhone initiating an automatic iCloud backup of its data to a known Wi-Fi network which may have obviated the need to unlock the phone and this subsequent litigation.[284]

Examining Apple's terminology in its court filings, Apple does not state that its assistance to unlock the phone would not have been needed had the FBI consulted with it first; it simply states "this litigation may not have been necessary."[285] Apple's discussion and focus on the change of the iCloud account password is, "a red herring" for a number of reasons. First, Apple does not deny that the device's passcode would need to be entered at least once after the device was powered on in order for there to be an automatic backup to the iCloud account. Second, Apple's public documents on this matter indicate a backup would not automatically occur because the device was found powered off, and was no longer set/linked to the iCloud backup.

According to Apple's iOS9.0 Security Guide, the passcode must be entered when the device has been restarted.[286] Thus, the passcode would be required once the device was turned back on. Also, according to Apple, "iCloud Backup occurs only when the device is locked, connected to a power source and has Wi-

---

281 Pluhar Supplemental Declaration, *supra* note 12, at 3.

282 Opposition, *supra* note 13, at 28; *see also id.* at 2; Perino Declaration, *supra* note 39, at 5.

283 Motion to Vacate, *supra* note 18, at 11 n.21.

284 *See id*. at 11.

285 *Id*.

286 *See iOS9.0 Security Guide*, *supra* note 45, at 7 ("The passcode […] is still required under the following circumstances: The device has just been turned on or restarted.").

Fi access to the Internet."[287] However, the iCloud backup also has to be setup.[288] In this case, the iPhone had been powered off and the iCloud backup had not occurred since October 19, 2015, indicating it was disabled.[289] Therefore, even with the powering on of the device, it would not automatically backup to the iCloud as the backup function would need to be reset which again requires the passcode. And, neither the FBI nor SBCDPH had the passcode. According to Apple's public papers, it is unlikely changing the password impacted the iCloud account. Thus, Apple's public documents support the DoJ/FBI, and one must remove how or why the iCloud password changed from the discussion.

Apple also argues, based upon a statement from the San Bernardino Police Chief, there is no need for the FBI to search the device as it is simply speculating the device contains valuable information related to the incident.[290] Apple's reliance on a statement from someone outside the FBI is misplaced and itself is speculative. There is evidence found on the iCloud account associated with the device that indicates the subject communicated with victims the day they were killed on December 2, 2015; and because the backup ended on October 19, 2015, the iCloud account would not have these communications. There are also toll records that show the subject communicated with his wife, who committed the terrorist attack with him, from July through November 2015. However, these communications are not found in the backup iCloud data. Although what data is maintained only on the device appears to be a matter of disagreement between the two parties, it also appears the iCloud account does not contain all data maintained on the device.[291] Thus, one may conclude the device contains critical data to the underlying terrorist event that is not located within the iCloud account. Finally, as to the FBI's need to contact various federal agencies to determine whether a particular agency is able to access the encrypted data, there is nothing within *N.Y. Telephone Co.* which even implies this is a requirement.

In examining this issue, one must focus on the language of the AWA statute, and it states "all courts . . . may issue all writs necessary or appropriate in aid of their respective jurisdictions."[292] Contrary to Apple's argument, the standard enunciated in the AWA does not require absolute necessity. However, here Apple's assistance is necessary. Thus, focusing on the statute's words, the DOJ

---

287 *Id.* at 42.

288 *How to back up your iPhone, iPad, and iPod touch*, APPLE SUPPORT, https://support.apple.com/en-us/HT203977 (last visited Feb. 9, 2018) (describing the steps one must take before automatic iCloud backup can occur).

289 Opposition, *supra* note 13, at 29-30; Pluhar Declaration, *supra* note 6, at 3; Pluhar Supplemental Declaration, *supra* note 12, at 3-4.

290 Reply, *supra* note 42, at 22.

291 *Compare* Pluhar Supplemental Declaration, *supra* note 12, at 4-5 (explaining what data Pluhar believes is maintained on the device and in the iCloud) *with* Neuenschwander Supplemental Declaration, *supra* note 125, at 9-10.

292 28 U.S.C. § 1651(a) (2012).

has a stronger argument as the statute only requires the writ be necessary for the court to avail itself of the AWA. In this case, the court's search warrant issued would be completely thwarted if Apple does not assist the FBI, and this basis (to ensure a court's jurisdiction is not completely thwarted) is consistent with case law.

VI. DOES THE ORDER VIOLATE APPLE'S FIRST AMENDMENT RIGHTS?

The First Amendment of the United States Constitution states "Congress shall make no law . . . abridging the freedom of speech."[293] When applying the First Amendment, the Supreme Court has acknowledged there is no constitutional difference between restricting one's speech and compelling one's speech.[294] Apple relies upon the First Amendment's application to compelled speech to argue the Government is violating its First Amendment right to not speak by ordering it to write computer code requiring its cryptographic signature and unique ID. And, because the compelled speech is contrary to Apple's views on privacy, it is viewpoint discrimination and requires the court's highest level of scrutiny.[295] The DOJ completely disagrees with Apple's First Amendment argument.

Before one can determine whether computer code is speech for First Amendment purposes, and if so, to what extent it is protected, one must first understand the basic concepts of computers and computer code. In support of its First Amendment argument, Apple cites *Universal City Studios Inc. v. Corley*[296]. While *Corley* examines the First Amendment's application to computer code, *Corley* (as well as its underlying district court cases) also provides fundamental concepts about computers and computer code (to include what is object code, what is source code, and the difference between the two) that is still applicable today and will prove helpful in determining whether code writing is speech for First Amendment purposes.

At its most basic level, computers function with a series of on-and-off

---

293 U.S. CONST. amend. I.

294 Riley v. National Fed'n of Blind, 487 U.S. 781, 796-97 (1988) ("There is certainly some difference between compelled speech and compelled silence, but in the context of protected speech, the difference is without constitutional significance, for the First Amendment guarantees 'freedom of speech', a term necessarily comprising the decision of both what to say and what not to say.").

295 Motion to Vacate, *supra* note 18, at 32-34.

296 Universal City Studies Inc., v. Corley, 273 F.3d 429, 445 (2d Cir. 2001), *aff'g sub. nom.* Universal City Studios Inc. v. Reimerdes (Universal I), 111 F. Supp.2d 294 (S.D.N.Y. 2000) and Universal City Studios Inc. v. Reimerdes (Universal II), 111 F. Supp.2d 346 (S.D.N.Y. 2001).

switches, using two digits in a binary (base 2) number system – 0 (for off) and 1 (for on). All data and instructions read by the computer must be reduced to the numerals 1 and 0. These strings of 0s and 1s are commonly referred to as object code. Fundamentally, a computer reads and translates everything into basic object code or a binary number set of bits (be it Base 64, ASCII, or Unicode). Computer language programs (JAVA, BASIC, C++, etc.) use symbols and syntax which is more commonly referred to as source code. In order for the computer to read and carry out the functions of the computer program language, the source code must be translated back into object code (strings of 0s and 1s). A compiler (internal to the computer) is the device/mechanism which translates the source code into object code (readable strings of 0s and 1s). A computer program's language, the source code, may contain more 1s and 0s (thus appearing more like object code) or the source code may contain more written text instructions (thus appearing more like a language). However, no matter whether the source code has more language than numbers (or more numbers than language), the computer's compiler must ultimately translate the source code into object code, strings of 0s and 1s.[297]

When trying to determine whether object code is speech for First Amendment purposes, and what, if any First Amendment protections apply to it, the following outline may prove helpful.

a. If the object code is not speech for First Amendment purposes, the analysis would end.

b. If the object code is speech for First Amendment purposes, then one must determine what level of scrutiny the court should apply based upon a determination as to whether the compelled speech is content-based or content-neutral (or possibly commercial speech).

c. If the object code combines speech and non-speech elements, then one must determine what level of scrutiny the court should apply?[298]

In this particular case, the DOJ wants the court to take the position that computer code is not speech, and no further analysis is required. On the other hand, Apple wants the court to take the position that all computer code is speech and therefore, First Amendment protections do apply (and would argue the highest level of scrutiny is required). The case law which examines computer programs and computer code has issued decisions based upon the particular,

---

297 *Id.* at 439-39 ("A computer responds to electrical charges, the presence or absence of which is represented by strings of 1's and 0's. Strictly speaking, 'object code' consists of those 1's and 0's […] Source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer. This task is usually performed by a program called a compiler.").

298 *See id.* at 449-51 (explaining how a court considers these various factors in determining whether computer code is speech for First Amendment purposes and is thus entitled to the protections of this Amendment).

unique facts of the case before it. Therefore, when answering the question whether computer code is protected by the First Amendment, the answer is: "it depends on the facts." One should also be mindful that the Supreme Court has not specifically addressed the question of whether computer code is protected under the First Amendment, and if so, to what extent?

Apple is correct that there is some case law that protects computer code as speech under the First Amendment; however, Apple implies all computer code is protected speech, and this implication is incorrect. Apple cites *Universal City Studios Inc. v. Corley* [299] in support of its argument that computer code is protected, and *Corley* does protect computer code and computer programs; however, *Corley* does not protect all computer code under the First Amendment, and specifically rejected the argument that all computer code is protected under the First Amendment.[300]

However, before one reviews *Corley*, one should examine the earlier case of *Commodities Futures Trade Commission ("CFTC") v. Vartuli*[301] ("*Vartuli*") as it examined the possible First Amendment application to computer programs and computer code and was relied upon by the *Corley* Court. In *Vartuli*, the Defendants marketed and sold a computer program, Recurrence, to buyers guaranteeing profits in currency futures. In challenging various CFTC charges, Vartuli, a developer of Recurrence, claimed the requirement to register as a commodity trading advisor was a prior restraint of speech on Recurrence, and therefore required the court's highest level of scrutiny.[302] The court rejected this argument and concluded Recurrence, as marked and sold, was not speech protected by the First Amendment[303] because the system was automatic, command-like. More specifically, the court wrote,

> The language at issue here was to be used in an entirely mechanical way, as though it were an audible command to a machine to start or to stop. 'The point . . . [was] not to convey information or to assert values.' It was to induce action without the intercession of the mind

---

299 *Id.* at 449-50 (discussing how the Second Circuit Court of Appeals concluded that some "computer code conveying information is 'speech' within the meaning of the First Amendment" and is thus entitled to its protections), *aff'g sub. nom.* Universal City Studios Inc. v. Reimerdes (Universal I), 111 F. Supp. 2d 294 (S.D.N.Y 2000) *and* Universal City Studios Inc. v. Reimerdes (Universal II), 111 F. Supp. 2d 346 (S.D.N.Y. 2001).

300 *Id.* at 451 ("Nevertheless, this momentary intercession of human action does not diminish the nonspeech component of code, nor render code entirely speech, like a blueprint or a recipe.").

301 Commodities Futures Trading Comm'n v. Vartuli, 228 F.3d 94, 111 (2d Cir. 2000) (explaining how the computer program Recurrence is not speech protected by the First Amendment).

302 *Id.* at 109.

303 *Id*. at 111.

> or the will of the recipient. None of the reasons for which speech is thought to require protection above and beyond that accorded to non-speech behavior—the pursuit of truth, the accommodation among interests, the achievement of social stability, the exposure and deterrence of abuses of authority, personal autonomy and personality development, or the functioning of a democracy—is implicated by the communications here in issue, and none counsels in favor of treating the Recurrence communications at issue as protected 'speech.' . . . In other words, the fact that the system used words as triggers and a human being as a conduit, rather than programming commands as triggers and semiconductors as a conduit, appears to us to be irrelevant for purposes of this analysis.[304]

While the *Vartuli* Court concluded, under its particular facts, the computer program Recurrence was not speech for First Amendment purposes, this did not mean all computer programs were not speech for First Amendment purposes.[305] And, in *Corley*, the Second Circuit was presented another opportunity to expand on its position of First Amendment application to computer programs and computer code.

The issues presented in *Corley* concerned digital versatile disk ("DVD") copyright and the constitutionality of the *Digital Millennium Copyright Act's*[306] ("*DCMA's"*) anti-trafficking provisions. The district court had issued an injunction against Corley permanently preventing him from posting the movie decryption (computer) program, de-Content Scramble System ("de-CSS"),[307] on its webpage or linking to another's website. De-CSS had originally been posted only in object code, computer readable string of 0s and 1s. The Defendant appealed the district court's injunction order under various constitutional arguments, to include the First Amendment.[308] When analyzing the First Amendment issues, the Second Circuit examined them as follows: (1) Is computer object code speech? (2) Are computer programs speech? (3) What is the First Amendment's scope of protection for computer object and source code? (4) What is the First Amendment's scope of protection for the decryption code, de-CSS?[309]

In examining the question as to whether computer object code is speech, the *Corley* Court first concluded that object code did not lose its constitutional

---

304 *Id*.

305 *See id.* at 112 (explaining that any statement made by a computer program should be "subjected to careful and particularized analysis to insure that no speech entitled to First Amendment protection fails to receive it.").

306 17 U.S.C. §1201(2)(A)-(C) (2012).

307 Content Scramble System ("CSS") is used by the movie industry to encrypt digital versatile disks.

308 *Universal City Studios, Inc.*, 273 F.3d at 436.

309 *Id*. at 445.

protection as speech simply because it is expressed in binary code.[310] The court drew an analogy to mathematical formulae and musical scores, both written in a form of code or symbolic notations that are not understood by all; however, both are covered by the First Amendment.[311] The court went on to say that if someone wrote a novel entirely in computer object code, the novel would be no different for constitutional purposes than if it had been written in English, and while a novel written in object code may only be read by a limited group of individuals, it would be no more incomprehensible than a novel written in Sanskrit.[312] Interestingly, the court acknowledged that a work of literature is unlikely to be written in a binary object code string as it is primarily the program language executed by a computer; however, it went on to say that "the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from conventional speech for First Amendment purposes, it is not because it is written in an obscure language."[313] In theory, the court's statements are accurate. If a novel were entirely written in binary code, only computer programmers would be able to read the novel; however, would computer programmers really read *War and Peace* written in binary code? One would suspect the answer to be "no." And, it is the code's function, or use, which is significant to both the *Vartuli* and *Corley* Courts when determining what code is protected by the First Amendment.

Appellant Corley had argued that all code should be protected in the same manner as an engineering blueprint or a recipe; however this position was rejected by the court.[314] The court examined the computer program object code's function which was a set of instructions to a computer either to perform a task or series of tasks when initiated by a click or series of clicks once a program is operational (or launched) to manipulate data that the user enters into the computer. Whether this object code that gives a computer instructions is speech within the meaning of the First Amendment requires consideration of the scope of the Constitution's protection of speech (content-based/content-neutral speech regulation, expressive activity/symbolic conduct, and non-speech and speech elements). The court concluded the "realities of what code is and what its normal functions are require a First Amendment analysis that treats code as combining non-speech and speech elements, i.e. functional and expressive elements."[315] The court also noted that before it could examine the level of protection, one

---

310 *Id*. at 445-46.
311 *Id*. at 447-48.
312 *Id*. at 445-46.
313 *Id*. at 446.
314 *Id*. at 451.
315 *Id*.

must identify what part of the regulated activity is "sufficiently imbued with elements of communication to fall with the scope of the First Amendment."[316] And once that speech component is identified, then one examines what level of scrutiny the court is to apply.

When the court examined the scope of the Constitution's protection of speech to object code, the *Corley* Court also acknowledged *Vartuli*, noting that it had considered two ways in which a programmer might be said to communicate through code: to the user of the computer program (in that case, Recurrence) which would not necessarily be protected, and *to the computer which was never protected*.[317] Thus, if object code that tells a computer what to do is not speech for First Amendment purposes, then it logically follows that being required to write object code, as directed in the Order, would not be compelled speech for First Amendment purposes. Thus, Apple's First Amendment argument (of compelled speech) is not supported by *Corley* and *Vartuli* because simply instructing a computer how to perform is not considered protected speech under the First Amendment.

While the code to be written is not being distributed, remains internal to the device (basically a minicomputer)[318] and simply tells the device/minicomputer how to function, Apple argues the expressive characteristics of code writing does satisfy elements of communication that warrant First Amendment protections. Apple also argues because the code to be written is cryptographically signed and contains a unique ID, these are indicia of speech requiring First Amendment protections. However, reading *Corley* and *Vartuli*, the signature and unique ID would be irrelevant to determining whether code writing is speech for First Amendment purposes. As to Apple's argument that there are expressive elements associated with code writing as code writers write code differently, even if one were to accept this argument, just as all expressive conduct is not automatically protected by the First Amendment,[319] not all expressive code writing should be protected by the First Amendment.

Case law concerning the First Amendment provides guidance to determine whether written code is constitutionally protected. For example, does the computer code, GovtOS/SIF, *convey information*[320] to a human being (which may be protected) as opposed to simply directing a device/minicomputer to function a particular way and is not protected?[321] Does the code contain any

---

316 *Id*. at 450.

317 *Id*. at 449.

318 Motion to Vacate, *supra* note 18, at 25 (Apple argues that an iPhone is really a minicomputer); *see infra* note 332 with accompany text.

319 *See* Texas v. Johnson, 491 U.S. 397, 406-07 (1989); Spence v. Washington, 418 U.S. 405, 409 (1974); United States v. O'Brien, 391 U.S. 367, 376-77 (1968).

320 *Universal City Studios Inc.*, 273 F.3d at 454.

321 *Id*.

expressive content[322] or an expressive purpose such as commentary, parody, news reporting, or criticism comprising of communicative messages by the author and/or operator that is not to the device/minicomputer?[323] Can you determine the speakers' purpose from the content of the communication?[324] One should be able to conclude that there is no expressive speech component in the development of GovtOS/SIF or computer code requiring First Amendment protection under the current DOJ–Apple facts. The conveyance of information is simply instructions to the device/minicomputer to disable (or enable) certain functional capabilities. The code stays internal to Apple and internal to the device. There is no audience, no public, and no person receiving the alleged speech. There is no message as the only purpose of GovtOS/SIF is to tell the device/minicomputer what to do. The Government is only requiring a functional outcome of the code. Thus, one may logically conclude GovtOS/SIF is a purely functional component of the computer code to be written and is not speech. Therefore, it is outside First Amendment protections.

VII. DOES THE ORDER IMPLICATE ANYONE'S FOURTH AMENDMENT RIGHTS?

The Fourth Amendment of the United States Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched . . . or things to be seized."[325] There is a tremendous amount of case law concerning what is a constitutionally appropriate search and seizure, and one recent case addressing the search of a smartphone is *Riley v. California*.[326] The issue presented in *Riley* was whether a search of a smartphone seized incident to a lawful arrest was permitted under the Fourth Amendment. The Court ultimately concluded the search of the smartphone incident to a lawful arrest violated the Fourth Amendment, and law enforcement is required to obtain a search warrant.[327]

In the current DOJ–Apple dispute, the DOJ's position is there are no Fourth Amendment issues raised under these particular facts as a court issued a probable cause search warrant (and the FBI obtained the owner's (SBCDPH's) consent to

---

322 *See* Name.Space, Inc. v. Network Solutions, Inc., 202 F.3d 573, 584-85 (2d. Cir. 2000).
323 *See id.* at 586.
324 *See* Hill v. Colorado, 530 U.S. 703, 721 (2000).
325 U.S. CONST. amend. IV.
326 Riley v. California, 134 S. Ct. 2473, 2484 (2014).
327 *Id.* at 2495.

search the device).[328] The DOJ recognizes the *Riley* decision and stated the FBI complied with *Riley* and obtained the search warrant.[329]

While Apple references *Riley*, its reference is not related to the search warrant requirement; rather its focus is on what a cell phone really is. "The term 'cell phone' is itself misleading shorthand . . . 'these devices are in fact minicomputers' that 'could just as easily be called cameras, video players, rolodexes, calendars, tape records, libraries, diaries, albums, televisions, maps, or newspapers.'"[330] Apple does not address a Fourth Amendment issue, either the terrorist's or anyone else's, albeit Apple would face a substantial hurdle if it tried, given the Court's discussion in *Alderman v. United States* outlining the general rule "that Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted."[331] The Supreme Court repeated the personal nature of Fourth Amendment rights, as well as noted its history of this recognition, in *Rakas v. Illinois*.[332] Thus, the DOJ's position that there are no Fourth Amendment issues is quite strong; Apple has no legal basis to assert anyone's (other than its own) Fourth Amendment rights.

VIII. DOES THE ORDER IMPLICATE ANYONE'S RIGHT TO PRIVACY?

When reviewing Apple's Motion to Vacate and Reply, one sees that Apple does not argue a specific individual's right to privacy or its own public position that "privacy is a fundamental human right."[333] Instead, Apple focuses on the privacy interests of all iPhone users or the public's privacy interests.[334] Apple's choice of terms is interesting, at least from an examination of constitutional protections. One must examine whose privacy interests are impacted. Does the Order's impact violate the deceased's right to privacy? A specific iPhone user, and if so, whose? all iPhone users' right to privacy? the public's right to privacy? Do any of these rise to the level of constitutional protections of a right to privacy? Is it appropriate for Apple to assert the constitutional rights of a specific individual, all iPhone users or the public?

In order to answer these questions, one must first determine where the right to privacy originates from? the Constitution? the common law? both? How far

---

328 Memorandum, *supra* note 70, at 2-3.
329 *See id*. at 2.
330 Motion to Vacate, *supra* note 18, at 25.
331 Alderman v. United States, 394 U.S. 165, 174 (1969).
332 Rakas v. Illinois, 439 U.S. 128, 140 (1978).
333 *Apple products are designed to protect your privacy*, *supra* note 80.
334 Motion to Vacate, *supra* note 18, at 1-2, 10 n.18; Reply, *supra* note 42, at 2, 13, 17, 20, 24 (describing how Apple did reference an individual's privacy interests in its March 15, 2016 motion when it stated "[w]e believe security shouldn't come at the expense of individual privacy.").

does the right of privacy, whether from the Constitution or common law, extend? The answers to these questions will then answer the questions as to whose right to privacy is being impacted and who can assert a violation of that right to privacy.

A. The Constitution and an Individual's Right to Privacy

Although the Constitution does not expressly confer a right to privacy, the Supreme Court has recognized an individual's right to privacy even when it has not directly correlated to a specific enumerated right in the Bill of Rights. In *Griswold v. Connecticut*,[335] the Supreme Court explained the right of privacy exists because "the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy. We have had many controversies over these penumbral rights of 'privacy and repose.'"[336] As indicated, *Griswold* was not the first case articulating the concept of penumbras surrounding the Bill of Rights. In *Olmstead v. United States*, a case pertaining to the application of the Fourth and Fifth Amendments to telephone wiretapping without a warrant, Justice Holmes, dissenting, recognized penumbras emanating from or surrounding the Fourth and Fifth Amendments.[337]

The Supreme Court again recognized the penumbra concept in *Whalen, Commissioner of Health v. Roe*, when it examined the issue of one's right to privacy versus a state's interest in collecting prescription data.[338] The Court acknowledged "[l]anguage in prior opinions . . . support . . . the view that some personal rights 'implicit in the concept of ordered liberty' are so 'fundamental' that an undefined penumbra may provide them with an independent source of constitutional protection."[339] While acknowledging the penumbra cases, the Court also expressed the opinion the right of privacy is founded in the Fourteenth Amendment's concept of personal liberty.[340] And, although there is at least one Supreme Court Justice who does not recognize a constitutional right to

---

335 Griswold v. Connecticut, 381 U.S. 479, 484 (1965); *see also* Wieman v. Updegraff, 344 U.S. 183, 196 (1952) (stating freedom of inquiry, freedom of thought, and freedom to teach); Martin v. City of Struthers, 319 U.S. 141, 143 (1943) (stating the fundamental right to distribute, the right to receive and the right to read); Pierce v. Soc'y of Sisters, 268 U.S. 510, 534-35 (1925) (stating the fundamental right of parents to educate their child in a school of choice: private, public or parochial); Meyer v. Nebraska, 262 U.S. 390, 403 (1923) (stating the fundamental right to study a particular subject or foreign language).

336 *Griswold*, 381 U.S. at 484-85.

337 Olmstead v. United States, 277 U.S. 438, 469 (1928) (Holmes, J., dissenting).

338 Whalen v. Roe, 429 U.S. 589, 598-99 n.23 (1977).

339 *Id*.

340 *Id*.

informational privacy,[341] there is ample case law to support the conclusion that individuals do have a constitutional right to privacy. However, for the deceased terrorist, he waived his privacy rights because SBCDPH had a written policy that the device could be searched at any time, and this policy was agreed to, in writing, when he accepted employment.[342]

B. The Constitution and a Corporation's Right to Privacy

The Supreme Court supports the conclusion that corporations do not have a general right to privacy. In *United States v. Morton Salt*,[343] the Court provided, "corporations can claim no equality with individuals in the enjoyment of a right to privacy"[344] albeit, corporations do have some rights which incorporate portions of privacy under the First, Fourth, Fifth, and Fourteenth Amendments.[345] The determining factor is:

> Corporate identity has been determinative in several decisions denying corporations certain constitutional rights, such as the privilege against compulsory self-incrimination, or equality with individuals in the enjoyment of a right to privacy . . . Certain 'purely personal' guarantees . . . are unavailable to corporations and other organizations because the 'historic function' of the particular guarantee has been limited to the protection of individuals. Whether or not a particular guarantee is 'purely personal' or is unavailable to corporations for some other reason depends on the nature, history, and purpose of the particular constitutional provision.[346]

Thus, given Apple's corporate identity and the history of the right to privacy, Apple does not have a general constitutional right to privacy.

C. The Common Law and the Right to Privacy

In examining the status of the common law right to privacy, the *Restatement*

---

341 *See* NASA v. Nelson, 562 U.S. 134, 169 (2011) (Thomas J., concurring in judgment) (citing McDonald v. Chicago, 561 U.S. 742, 811 (2010)) (Thomas J., concurring in part and concurring in judgment) (Justice Clarence Thomas wrote, "'I can find neither in the *Bill of Rights* nor any other part of the U.S. Constitution a general right of privacy … And the notion that the Due Process Clause of the Fifth Amendment is a wellspring of unenumerated rights against the Federal Government 'strains credulity for even the most casual user of words.'").

342 Application, *supra* note 6, at 3 n.1; Motion to Compel, *supra* note 11, at 5 n.4; Opposition, *supra* note 13, at 1.

343 United States v. Morton Salt Co., 338 U.S. 632, 652 (1950).

344 *Id*.

345 First Nat. Bank of Bos. v. Bellotti, 435 U.S. 765, 779 n.14 (1978).

346 *Id*.; *see also* Browning-Ferris Indus. Of Vermont, Inc. v. Kelco Disposal, Inc., 492 U.S. 257, 284-85 (O'Conner J., dissenting in part).

of Law, Second, Torts, § 652A identifies the four violations to one's right to privacy which are the following:

> (1) Intrusion Upon Another Person's Seclusion: One who intentionally intrudes upon another's solitude or seclusion (physical or otherwise) concerning his/her private matters if the intrusion would be highly offensive to a reasonable person.[347]
> (2) Appropriation of Another Person's Name or Likeness: One who appropriates for his/her own use or benefit (not limited to a commercial benefit) another's name or likeness. While analogous to copyright, it is not limited by copyright laws.[348]
> (3) Publicity Given to Another Person's Private Life: One who publicizes a matter pertaining to another's private life, if that publicized matter is such that it would be highly offensive to a reasonable person and is not a legitimate concern to the public.[349]
> (4) Publicity Placing Another Person in a False Light (this cause is not limited to defamation, but can be in addition to or separate from defamation): One who has publicized another person in such a manner that the false light of the other person would be highly offensive to a reasonable person, and the person/one had knowledge or acted in disregard to the falsity in which the other person would be placed.[350]

The *Restatement of Law, Second, Torts*, § 652G also identifies characteristics of the common law right to privacy which includes its personal nature (i.e. it is not assigned or maintained by another to include the individual's family, unless their own privacy is invaded), nor does it survive the death of the individual (in the absence of a statute). In addition, corporations do not have a right to privacy, and therefore have no cause of action for any of the four violations of privacy, with a caveat that a corporation has limited protections regarding its name or identity (from a competition perspective).[351]

Thus, one may conclude the deceased terrorist has no common law right to privacy in the device as any possible common law right to privacy ended upon his death, nor could a third party assert his right to privacy.[352] The deceased terrorist had also waived his privacy rights with his employer, SBCDPH.[353]

---

347 RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).
348 *ID*. § 652C.
349 *ID*. § 652D.
350 *ID*. § 652E.
351 *ID*. § 652G.
352 *See* CAL. CIV. CODE §3344.1 (2018) (California restricts the use of a deceased personality, name, voice, signature, photograph or likeness, in any manner, on in products or merchandise or goods, or for the purpose of advertising, or selling or promotion of such items unless specified approval is obtained.).
353 Application, *supra* note 6, at 3 n.1; Motion to Compel, *supra* note 11, at 5 n.4, 18 n.7;

Given the common law right to privacy does not extend to corporations, Apple and Apple's corporate users/customers would not have a common law right to privacy.[354] If an iPhone is limited to business purposes only, that information theoretically belongs to the corporation, not the individual, and the corporation does not possess the common law right to privacy.

Apple did raise the issue of the "privacy interests" of all other iPhone owners.[355] Accepting that corporations do not have a common law right to privacy, the question then is whether Apple has standing to assert this cause of action on behalf of these individuals (assuming it can separate individuals from non-individuals). Given the restriction that the common law right to privacy is personal, one could conclude that Apple cannot assert the common law right to privacy on behalf of all other individual iPhone users.

D. Standing to Assert a Constitutional Right to Privacy

The Supreme Court recently articulated principles and requirements of federal-court jurisdiction and standing. In *Clapper v. Amnesty Int'l.*,[356] the Court recognized there is "'[n]o principle more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.'"[357] And, a corollary to that principle is the plaintiffs must establish they have standing to bring that case or controversy. Thus, could all other iPhone users who possess the personal right to privacy bring suit against the Government arguing the court's order that Apple create GovtOS/SIF violates their constitutional right to privacy? In the alternative, could Apple assert the constitutional violation on behalf of all other individual iPhone users not party to the litigation?

1. Standing and the Individual's Right to Privacy

According to *Clapper* and *Spokeo Inc. v. Robins*,[358] based upon demonstrated facts, the plaintiffs have the burden of establishing standing by satisfying the following three elements:

(a) Plaintiffs have suffered an injury-in-fact such that one has "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and

---

Opposition, *supra* note 13, at 1.

354 FCC, et al. v. AT&T Inc. et al., 131 S. Ct. 1177, 1185 (holding that "personal privacy" does not encompass corporations).

355 *Apple products are designed to protect your privacy*, *supra* note 80.

356 Clapper v. Amnesty Int'l, 568 U.S. 398, 401 (2013).

357 *Id*. at 408.

358 Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

'actual or imminent, not conjecture of hypothetical.'"[359] The Court further explains the articulated qualifying phrases. For an injury (1) to be particularized, it "'must affect the plaintiff in a personal and individual way;"[360] (2) to be concrete, it "must be '*de facto*'; that is, it must actually exist";[361] and (3) to be imminent, although an elastic concept, "it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative . . . [rather] the injury is *certainly* impending."[362] The Court further explained that *certainly* impending does not include allegations of a *possible* future injury or a chain of speculative possibilities of an injury at some indefinite future time.[363] And, even if there was an objective, reasonable likelihood the injury would occur, this would still not satisfy the *certainly* impending requirement.[364]

(b) The injury-in-fact "is fairly traceable to the challenged conduct of the defendant."[365]

(c) The injury-in-fact "is likely to be redressed by a favorable judicial decree."[366]

Applying these three elements to all other iPhone users as potential plaintiffs, Apple faces a number of obstacles detrimental to its ability to meet standing requirements. First, potential plaintiffs could only be those that have a recognized personal right to privacy. Again, if an iPhone is limited to business purposes only, that data/information theoretically belongs to the corporation which does not possess the general (constitutional) personal right to privacy. So, "all other iPhone users" could not meet this first prong. Second, if the remaining iPhone users (those that can assert a general right to privacy) assume Apple's argument of the impact of GovtOS/SIF to their iPhones, it would be difficult to establish a concrete injury-in-fact, a violation of their right to privacy to their specific devices. Apple's arguments are built on a chain of events that are speculative, hypothetical and too remote, particularly as to whose iPhone becomes vulnerable to access, when the iPhone would be accessed, and who could inappropriately access the device. One cannot simply fear their iPhone would be inappropriately accessed or hacked at some unknown time in the future and consider that fear a violation of their right to privacy. In addition, one cannot establish standing by incurring expenses to prevent the inaccessible access or

---

359 *Id*.
360 *Id*.
361 *Id*.
362 Clapper v. Amnesty Int'l, 568 U.S. 398, 409 (2013) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).
363 *Id*. at 409.
364 *Id*. at 410.
365 Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
366 *Id*.; *see also* Phillips Petroleum Co. v. Shutts, 472 U.S. 797, 804 (1985).

hacking as one would be inflicting harm on oneself based on fears of a hypothetical future and unknown event.[367]

There are data breach cases which address the issue of standing and a fear of identity theft. Cases where the plaintiffs have not met the standing requirements due to the speculative nature of the injury include *Reilly v. Ceridian*[368] and *Beck v. McDonald*.[369] Alternatively, there are other data breach cases where standing requirements have been met, such as, *Horizon Healthcare Services Inc. v. Data Breach Litigation*.[370] Recent cases also recognize a circuit split is occurring regarding satisfaction of the standing requirements in data breach cases.[371] While there may be cases with different standing results, one thing they have in common is they set out the requirements to establish standing, and then focus on how a specific event is to occur and by whom. When these variables are unknown and indefinite, standing is not found. In the DOJ–Apple dispute, who will breach GovtOS/SIF, when will they breach it, how they will breach it, and what iPhones will be breached are all unknown, indefinite events. Thus, it would be difficult for those iPhone users who have the personal right to privacy to establish standing.

2. Standing and Jus Tertii

Some commentators have argued Apple should assert the constitutional rights of non-litigant iPhone users under the concept of *jus tertii*.[372] Thus, one must ask whether Apple would have standing to assert a violation of all iPhone users' constitutional right to privacy. This is in contrast to the general rule that "a litigant must assert his or her own legal rights and interests, [sic] and cannot rest a claim to relief on the legal rights or interests of third parties."[373] However, as

---

367 *Clapper*, 568 U.S. at 416.

368 Reilly v. Ceridian, 664 F.3d 38, 41 (3d Cir. 2011).

369 Beck v. McDonald, 848 F.3d 262, 267-68 (4th Cir. 2017).

370 Horizon Healthcare Services Inc. v. Data Breach Litigation, 846 F.3d 625, 629 (3d Cir. 2017).

371 *See* Katz v. Pershing LLC, 672 F.3d 64, 80 (1st Cir. 2012); Fero v. Excellus Health Plan, Inc., 304 F.Supp.3d 333, 340-41 (N.Y.W.D. 2018).

372 Robert Fein, *How Apple Could Best the FBI*, U.S. NEWS & WORLD REPORT (Feb. 22, 2016, 12:15PM), https://www.usnews.com/opinion/articles/2016-02-22/apple-may-not-have-a-right-to-privacy-but-its-iphone-customers-do (explaining that jus tertii is a Latin term that mean a right of a third party which allows one party to argue that another parties' rights are at state); Eugene Goroshko, *Crypto-War: What is it Good For?: The FBI's Legal Battle with Apple Encryption…is Over!*, THE DECISIVE UTTERANCE (Apr. 4, 2016), https://decisiveutterance.jmls.edu/2016/04/04/crypto-war-what-is-it-good-for-the-fbis-legal-battle-with-apple-over-encryption-is-over/; Ashley Shaw, *What is Going on With Apple and the FBI?*, PASHA L. (Feb. 23, 2016) https://www.pashalaw.com/apple-fbi/.

373 Powers v. Ohio, 499 U.S. 400, 410 (1991); *see also* Barrows v. Jackson, 346 U.S. 249, 255 (1953).

the commentators have noted, the Court has permitted exceptions to the general rule[374] and thus, the question must be analyzed.

When examining the possible use of *jus tertii*, one must consider the following three principles: The first principle is that it is an exception to the general rule and the second is that courts are cautious in allowing others to vindicate the constitutional rights of non-litigants. Reasons include: Not all individuals who possess the constitutional rights want them asserted; non-litigants will be able to enjoy them regardless of whether the in-court litigant is successful or not; and each individual is generally the best or most effective advocate and in the best position to assert his or her own rights.[375] The third principle is "the limitations on a litigant's assertion of *jus tertii* are not constitutionally mandated, but rather stem from a salutary 'rule of self-restraint' designed to minimize unwarranted intervention into controversies where the applicable constitutional questions are ill[-]defined and speculative."[376] Thus, for the Court, a litigant's limited ability to use *jus tertii* is a prudential rule that has not been enforced when the underlying justifications for the general rule are absent.[377]

One such case is *Barrows v. Jackson*, where the Court provided one type of *jus tertii* outline to determine whether a seller of property, bound by a restrictive covenant to sell only to Caucasians, could assert the constitutional rights of potential buyers. The Court first questioned whether the damage award imposed on the seller for violating the restrictive covenant was state action for Fourteenth Amendment purposes. After concluding that it was state action for Fourteenth Amendment purposes,[378] the Court's second question was whether the state's allowance for a damage award for failure to comply with a restrictive covenant deprived anyone of their constitutional rights. The Court specifically found that, solely based upon race, potential non-Caucasian buyers were unable to purchase land on the same terms as Caucasians.[379] The Court then asked whether the seller could assert of the constitutional rights of the potential buyers, ultimately concluding the seller could.[380]

In later *jus tertii* cases, the Court loses focus on the first two questions, and

---

374 Caplin & Drysdale v. United States, 491 U.S. 617, 623 n.3 (1999); *see Powers*, 499 U.S. at 414; Craig v. Boren, 429 U.S. 190, 193-97 (1976); Singleton v. Wulff, 428 U.S. 106, 113-14 (1976); Eisenstadt v. Baird, 405 U.S. 438, 438 (1972); NAACP v. Alabama, 357 U.S. 449, 449 (1958) *rev'd on other grounds*, 360 U.S. 240 (1959); *Barrows*, 346 U.S. at 255-56.

375 *See Singleton*, 428 U.S. at 113-14.

376 *Craig*, 429 U.S. at 193.

377 *Singleton*, 428 U.S. at 114.

378 *Barrows*, 346 U.S. at 254.

379 *Id*.

380 *Id.* at 254-55.

primarily places its emphasis on question three, stating that it is appropriate for a litigant to assert the constitutional rights of a non-litigant when the following three elements are met:

"[1] the litigant must have suffered an 'injury in fact,' thus giving him or her a 'sufficiently concrete interest' in the outcome of the issue in dispute."[381] Other courts have asked whether the litigant has suffered some injury-in-fact adequate to satisfy Article III's case or controversy requirement.[382]

[2] the litigant must have a close relation to the third party; and

[3] there must exist some hindrance to the third-party's ability to protect his or her own interest.[383]

In reviewing the later *jus tertii* cases, the Court does not consistently articulate the *jus tertii* elements; however, the substantive, consistent analysis of the elements occurs. Later *jus tertii* cases establish the elements as follows:

(1) The litigant must have suffered some type of injury in fact to meet *Article III* requirements. For example, assessed monetary damages of $11,600 for violating the restrictive covenant of selling only to Caucasians;[384] the NAACP's loss of membership and financial aid if its membership list was released;[385] criminal conviction and imprisonment;[386] loss of income;[387] loss of sales, loss of liquor license and sanctions;[388] and loss of integrity within the judicial process, including in the defendant's trial.[389]

(2) The litigant must have a close relationship with the third-party, e.g., an attorney-client relationship[390] or doctor-patient relationship.[391] However, this element is not limited to these special, confidential relationships. Other cases rely upon the litigant being an effective advocate or whether the litigant and non-litigant are almost identical. For example, in *Barrows*, the litigant and seller of property was allowed to assert prospective buyers' constitutional rights as the seller was the only effective advocate.[392] In *NAACP v. Alabama*, the NAACP was permitted to assert its members' Fourteenth Amendment rights as it and its members were basically identical.[393] In *Eisenstadt v. Baird*, the relationship was

---

381 Powers v. Ohio, 499 U.S. 400, 411 (1991).
382 Caplin & Drysdale v. United States, 491 U.S. 617, 623 n.3 (1989).
383 *Powers*, 499 U.S. at 411, (citing Singleton v. Wulff, 428 U.S. 106, 115-116 (1976)).
384 *Barrows*, 346 U.S. at 255.
385 NAACP v. Alabama, 357 U.S. 449, 451, 460 (1958), *rev'd on other grounds*, 360 U.S. 240 (1959).
386 Eisenstadt v. Baird, 405 U.S. 438, 446 (1972).
387 *Caplin & Drysdale*, 491 U.S. at 623 n.3 (citing *Singleton*, 428 U.S. at 113-118).
388 Craig v. Boren, 429 U.S. 190, 195 (1976).
389 Powers v. Ohio, 499 U.S. 400, 411, 413 (1991).
390 *Caplin & Drysdale*, 491 U.S. at 623 n.3 (citing *Singleton*, 428 U.S. at 113-118).
391 *Singleton*, 428 U.S. at 113-118; Griswold v. Connecticut, 381 U.S. 479, 481 (1965).
392 Barrows v. Jackson, 346 U.S. 249, 259 (1952).
393 NAACP v. Alabama, 357 U.S. 449, 459-60 (1958), *rev'd on other grounds*, 360 U.S.

not that of "a distributor and potential distributees, but that between an advocate of the rights of persons to obtain contraceptives and those desirous of doing so."[394] The Court also asked whether the non-litigant's rights are diluted or adversely affected if their rights cannot be asserted by the litigant. For example, whether Eisenstadt was successful or not, one would not be able to purchase or obtain contraceptives.[395] In *Craig v. Boren*,[396] the relationship was not of vendor of alcohol and potential buyers, but that of an advocate for those seeking access to that vendor's market.[397] The Court also examined what impact there was to the non-litigant's rights.[398] Relying upon *Eisenstadt*, the *Craig* Court concluded that males between the ages of 18-20 would be materially impacted in their ability to purchase beer irrespective of whether the vendor was successful in the claim against the State.[399] In *Powers v. Ohio*, the Court went back to the litigant being fully, or very nearly, as effective a proponent of the constitutional right as the non-litigant.[400]

(3) Is there some hindrance to the ability of the third party to assert his own right? In *Barrows*, the Court simply concluded it would be impossible for buyers to assert their constitutional claim.[401] In *NAACP v. Alabama*, while also impossible, the Court noted that if members asserted their claim, it nullified their constitutional right of association.[402] Other impacts include a chilling effect and the publicity associated with being named in litigation concerning family planning matters falling within the doctor-patient relationship.[403] In *Powers*, it was the probability and inability of the third-parties to assert their own rights because the potential jurors would face barriers in obtaining the underlying jury selection information and would face a significant economic burden if litigated.[404]

Barrows and *Power* both provide guidance to determine whether it is appropriate for Apple to use the *jus tertii* exception and assert the constitutional rights of non-litigants.

The first issue is whether Apple has suffered an injury-in-fact that would satisfy Article III's case or controversy requirements. Although Apple has no

---

240 (1959).

394 Eisenstadt v. Baird, 405 U.S. 438, 445 (1972).

395 *Id*. at 464.

396 Craig v. Boren, 429 U.S. 190, 195 (1976).

397 *Id*.

398 *See* Singleton v. Wulff, 428 U.S. 106, 114-15 (1976).

399 *Craig*, 429 U.S. at 196.

400 Powers v. Ohio, 499 U.S. 400, 413 (1991) (citing *Singleton*, 428 U.S. at 115).

401 Barrows v. Jackson, 346 U.S. 249, 259 (1953).

402 *Alabama*, 357 U.S. at 459-60.

403 Griswold v. Connecticut, 381 U.S. 479, 481-82 (1965); *Singleton*, 428 U.S. at 117.

404 *Powers*, 499 U.S. at 414-15.

common-law or general constitutional right to privacy, it could argue that its products would be less secure and would not be purchased, theoretically resulting in a loss of revenue. Granted, this may be speculative given that iPhones were purchased pre-iOS8 when data was not encrypted; however, assuming Apple is able to satisfy Article III's case or controversy requirements, then one may proceed to *Barrows'* second question.

The next issue is whether the court order, denies individual iPhone users their constitutional (general) right to privacy. It is doubtful that individual iPhone users who possess a general right to privacy could meet the standing requirements of any potential breach to their iPhones. Therefore, the Government's actions do not deprive anyone of their constitutional right to privacy. And, if individual iPhones users are unable to establish a violation of their constitutional rights because of standing, Apple should not be able to assert a constitutional violation on their behalf.

Additionally, it is clear there is no confidential relationship equivalent to a doctor-patient or attorney-client relationship between Apple and all individual iPhone users. In addition, Apple takes great pains in distancing itself from its customers in order to distance itself from the device at issue. However, Apple could argue it is acting as an advocate of all individual iPhone users, and Apple would be as effective in protecting their rights as they would be. However, do all individual iPhone users want Apple to assert their general right to privacy, or are there iPhone users who want Apple to assist the FBI without considering this issue as an impact on their right to privacy. There is a reasonable likelihood that there are iPhone users who want Apple to assist the FBI and do not see an impact to their right to privacy or consider it too speculative.

There seems to be no chilling effect, embarrassment or nullification of one's rights that would be of concern to a court with regards to a third-party's ability to protect his or her own interest. Probably the most significant hindrance is cost of any litigation; however, given the number of amicus briefs that were filed, one could argue that third-party interests are already being protected.

In sum, in spite of the commentators' suggestion that Apple use the concept of *jus tertii*, Apple would have difficulty in establishing some of the required elements; thus it does not appear to be a realistic option.[405]

---

[405] *See* Dep't of Labor v. Triplett, 493 U.S. 715, 720 (1990) (some commentators have argued that Apple should argue *jus tertii* and iPhone user's Fourth Amendment rights; however, given the personal nature of the right, this author chose not to include it in the discussion of *jus tertii*, and limited the discussion to the constitutional right to privacy.); United States v. Payner, 447 U.S. 727, 731-32 (1980); Rakas v. Illinois, 439 U.S. 128, 143 (1978); *Barrows*, 346 U.S. at 259-60; s*ee also* notes 327-334 with accompany text.

IX. DOES THE COURT ORDER VIOLATE APPLE'S FIFTH AMENDMENT RIGHTS?

The Fifth Amendment states, "No person shall be . . . deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation." [406] In its Motion to Vacate, Apple argues the Government has violated its Fifth Amendment right to due process because it has been conscripted to provide services to the Government against its will.[407] Although not specifically raised as a violation of due process, Apple implies a due process violation when the DOJ filed its Application and obtained the Order without any notice or opportunity to be heard given to Apple.[408] The DOJ disagrees with Apple's arguments and/or implications.

A. The DOJ's Ex Parte Application

In its Motion to Vacate, Apple implies the DOJ acted improperly "by invoking 'terrorism' and moving *ex parte* behind closed doors . . . cut[ting] off debate, and circumvent[ing] thoughtful analysis."[409] Apple also implies the court should not have signed the *Order*, writing "[w]ith no opposition or other perspectives to consider, the [c]ourt granted the government's request and signed the government's proposed order." [410] Apple's argument is rather interesting given many of the cases it cites are situations where the AWA order was obtained via an *ex parte* application.[411] It is noted that one case required the AWA order be modified to provide the third-party a time period to object to the order; however, the order was issued via an *ex parte* application.[412] Even in *N.Y. Telephone Co.*, the court's order was pursued via an *ex parte* application. [413] Clearly, the DOJ's actions are consistent with other AWA cases in terms of requesting an AWA order through an *ex parte* application, and the February 16, 2016 *Order* gave Apple five business days to seek relief from the court if Apple believed complying with the *Order* would be unreasonably burdensome.[414] Thus, one may conclude the DOJ did not act improperly when it filed the *ex parte* application.

---

406 U.S. CONST. amend. V.
407 Motion to Vacate, *supra* note 18, at 34; Reply, *supra* note 42, at 25.
408 Motion to Vacate, *supra* note 18, at 11 n.22.
409 *Id.* at 2.
410 *Id*. at 12.
411 *See id.* at pp. i-iv.
412 *See In re Order XXX, Inc.,* 2014 U.S. Dist. LEXIS 154743, at *5 (S.D.N.Y. Oct. 31, 2014).
413 United States v. N.Y. Tel. Co. 434 U.S. 159, 172 (1977).
414 Order, *supra* note 28, at 3.

B. Did the Government Conscript Apple?

In its Motion to Compel, the DOJ states it "does not seek to deny Apple its right to be heard,"[415] and given Apple's public position of litigation and its intent to not comply with the Order, it filed its "motion to provide Apple with the due process and adversarial testing it seeks."[416] Thus, one may conclude the DOJ not only wanted to ensure Apple was not denied due process, it wanted to affirmatively ensure that Apple was given due process.

The DOJ's perspective of due process is one of notice and opportunity to be heard, and given how Apple has legally challenged the DOJ, one must agree with the DOJ's statement that "it is ludicrous to describe the government's actions here as 'arbitrary.'"[417] The DOJ does address Apple's substantive due process argument by stating,

> If Apple is asking for a *Lochner*-style holding that businesses have a substantive due process right against interference with its marketing strategy or against being asked to develop source code, that claim finds no support in any precedent let alone . . . [in] 'the concept of ordered liberty' or 'this Nation's history.'[418]

Thus, according to the DOJ, Apple's Fifth Amendment due process rights have not been violated.

Apple's substantive due process perspective is the denial of its liberty as the Government has "conscript[ed] a private party with an extraordinarily attenuated connection to the crime to do the government's biding in a way that is statutorily unauthorized, highly burdensome, and contrary to the party's core principles."[419] Additionally, the Government has conscripted Apple by requiring it "to send individual citizens into a super-secure facility to write code for several weeks on behalf of the government on a mission that is contrary to the values of the company and these individuals."[420] And, this conscription is a significant threat to the independence and liberty of Apple and its employees,[421] which violates Apple's Fifth Amendment due process rights.

From a notice due process perspective, one must conclude the DOJ has the stronger argument that Apple has received the required due process of notice and opportunity to be heard. Which leads to the conscription/substantive due process argument. While most associate conscription with a military draft, conscription is defined as "forc[ing] someone to work as a member of a

---

415 Motion to Compel, *supra* note 11, at 3.
416 *Id.* at 3 n.3
417 *See* Opposition, *supra* note 13, at 34.
418 *See id.* at 35.
419 Motion to Vacate, *supra* note 18, at 34.
420 Reply, *supra* note 42, at 25.
421 *Id*.

group."[422] Therefore, one must ask whether Apple is being forced to work with the FBI? Apple is simply writing code for a brief period of time so that the FBI can access the device. Writing the code is done without the FBI's involvement or supervision. In fact, Apple could simply turn over GovtOS/SIF to the FBI so that it can use GovtOS/SIF independently from Apple. Apple is either down-playing or ignoring the court's original jurisdictional authority, the probable cause search warrant, the historical authority behind the AWA, and how courts have recognized its authority throughout the AWA's more than 215-plus years of legal history. Thus, the DOJ also has the stronger substantive due process argument.

X. HAS ANYTHING CHANGED SINCE MARCH OF 2016?

The DOJ–Apple dispute remains unresolved since the February 16, 2016 Order was vacated on March 29, 2016, when the DOJ's filed notice to the court that it had been able to access the device.[423] It is rather ironic that once the FBI had access to the encrypted data, Apple wanted the FBI to tell them how it was done. The FBI declined to do so.[424]

On February 9, 2018, it came to light that Apple's iOS9 iBoot source code was leaked and made publicly available, for a brief period of time.[425] Apple's responded that "the leak wouldn't impact iPhone security for most users"[426] because iOS9.0 was three years old and had since been updated.[427] Although the iOS system has been updated, it is unclear whether the iBoot source code has been changed within each system, or how damaging this leak is to Apple. Does one really expect Apple to concede the leak impacted the security of its devices?

In February 2018, Forbes Magazine noted Cellebrite, a Government contractor, could break the encryption on all models of iPhones, from iOS5 to

---

422 *Conscript*, WEBSTER'S ENCYCLOPEDIA UNABRIDGED DICTIONARY OF THE ENGLISH LANGUAGE (2d 1993).

423 Final Order, supra note 4, at 25.

424 Alina Selyukh, *FBI Explains Why It Won't Disclose How It Unlocked iPhone*, NPR (Apr. 27, 2016, 5:44 PM), https://www.npr.org/sections/alltechconsidered/2016/04/27/475925946/fbi-explains-why-it-wont-disclose-how-it-unlocked-iphone.

425 Lorenzo Franceschi-Bicchierari, *How a Low-Level Apple Employee Leaked Some of the iPhone's Most Sensitive Code*, MOTHERBOARD (Feb 9, 2018, 3:38 PM), https://motherboard.vice.com/en_us/article/xw5yd7/how-iphone-iboot-source-code-leaked-on-github.

426 Conner Forrest, *Apple iBoot leak was an inside job, and the hacker has more iOS source code*, TECHREPUBLIC (Feb. 12, 2018, 3:38 PM), https://www.techrepublic.com/article/apple-iboot-leak-was-an-inside-job-and-the-hacker-has-more-ios-source-code/.

427 Tom Spring, *Apple Downplays Impact of iBoot Source Code Leak*, THREATPOST (Feb. 8, 2018, 5:26 PM), https://threatpost.com/apple-downplays-impact-of-iboot-source-code-leak/129852/.

iOS11.[428] Both of these events could have put a dent in Apple's arguments that assisting the Government would damage the security of its products and the privacy of its customers. However, Apple's argument could be revived because Apple is continuously striving to protect its products, and could have developed additional protocols to further protect its products.

In June 2018, Apple announced it would change its iPhone settings to prevent companies like Cellebrite from circumventing its password limitations. According to reports by Reuters, "[Apple] was aiming to protect all customers, especially in countries where phones are readily obtained by police or by criminals with extensive resources, and to head off further spread of the attack technique."[429] While Apple added that it does not design its security improvements to frustrate law enforcement,[430] Apple's actions demonstrate the circular cycle of encryption and security. Circumvention by law enforcement or other third parties, and updates to encryption and security prolongs the dispute between Apple and the DOJ. Thus, from a legal perspective, it would appear that little has changed.

XI. CONCLUSION

Apple's encryption and non-encryption security features and the FBI's need to conduct a national security/law enforcement investigation is an issue that has yet to be resolved and still exists today.[431] The 2016 DOJ–Apple dispute was contentious, with no compromise between the two parties. Throughout the 43-day public legal dispute,[432] it was difficult to determine what was truly required of Apple, whether it was legally appropriate, and who had the stronger legal position. This article was an attempt to examine, and answer these questions. In sum, the DOJ seems to have the stronger legal arguments in the following areas:

(1) The Government has not violated Apple's Fifth Amendment due process

---

428 Thomas Brewster, *The Feds Can Now (Probably) Unlock Every iPhone Model In Existence*, FORBES (Feb. 26, 2018, 10:28 AM), https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#1c7a4ebf667a; *see also* Brandon Vigliarolo, *This company can hack every iPhone in the world*, TECHREPUBLIC (Feb. 27, 2018, 11:25 AM), https://www.techrepublic.com/article/this-company-can-hack-every-iphone-in-the-world/.

429 Joseph Menn, *Apple to undercut popular law-enforcement tool for cracking iPhones*, REUTERS (June 13, 2018, 4:16 PM), https://www.reuters.com/article/us-apple-iphone-cracking/apple-to-undercut-popular-law-enforcement-tool-for-cracking-iphones-idUSKBN1J92ZY.

430 *Id*.

431 *See* Thomas MacMillian, *Battle Between Police and Tech Firms Intensifies Over Smartphone Access*, WALL ST. J. (Nov. 27, 2017), https://www.wsj.com/articles/battle-between-police-and-tech-firms-intensifies-over-smartphone-access-1511827189.

432 Weise, *supra* note 1.

rights as Apple has been given notice and an opportunity to be heard; nor has the Government violated Apple's substantive due process rights as Apple has not been denied its constitutional liberties.

(2) The Government has not violated Apple's First Amendment rights as writing code that instructs a computer how to function is not speech under the First Amendment.

(3) The Government has not violated the Fourth Amendment as the FBI obtained a probable case search warrant and the owner of the device consented to the FBI's search of the device. As to alleged violations of third-parties' Fourth Amendment rights, as they are personal to the third-parties, Apple is not able to assert those rights on their behalf.

(4) Apple and corporate iPhone users do not have a common law or constitutional (general) right to privacy.

(5) Apple is not able to assert a common law right to privacy on behalf of other iPhone users who possess the right to privacy as it is personal to that individual.

(6) As to Apple asserting a violation of iPhone users' constitutional right to privacy (or Fourth Amendment rights assuming one could overcome the personal nature of those rights) under the legal theory of *jus tertii*, it is unlikely Apple would be able to meet the requirements of *jus tertii* as the injury-in-fact to individual iPhones users is too speculative.

(7) The court did not exceed its jurisdictional authority when it issued the *Order* given the court's underlying jurisdictional authority of the probable cause search warrant.

(8) CALEA is not a statute that directly addresses the issue before the court as CALEA applies to data in motion and not data at rest and is thus inapplicable.

Given the court's underlying jurisdictional authority and the AWA's 215-plus years of history, the focus of the DOJ–Apple dispute centers on whether the court properly used the AWA when it issued the Order, and whether the court properly analyzed the three elements articulated in *N.Y. Telephone Co.* for requiring third party assistance. The DOJ has the stronger argument for two of those prongs (Apple is not too far removed and Apple's assistance is necessary). The primary legal issue centers on the second prong and whether the Order is burdensome or unreasonable. This issue is directly tied to the question whether the Order requires Apple to create a backdoor, a master key, and/or something equivalent to a master key. Because neither party provides definitions and the Declarations lack clarity as to how significant the modification to GovtOS/SIF must be in order for it to work on other iPhones, it cannot be determined whether the Order is unreasonable or burdensome. In order to resolve this issue, additional information is required, to include an accepted definition of backdoor

and master key and the extent of the modifications to GovtOS/SIF such that it would work on other iPhones.

It is clear the data encryption dispute is not going to go away, and the debate between national security and/or law enforcement investigations versus privacy and security of electronic devices has been, is, and will continue to be contentious. However, this author is of the opinion that it does not have to be polar positions in that one must completely give way to the other. Law enforcement agencies and technology companies can, and must, work together to protect the privacy interests of individual iPhone users (and the security of iPhones) as well as protect national security and law enforcement interests. Further litigation and new laws do not always truly solve the underlying issue between two important but competing interests. In fact, sometimes they may even create new issues not foreseen, especially in the digital world where new technological developments are occurring at a speed most cannot comprehend. In order to move from one's polar position, each party must understand and accept that if national security and law enforcement interests are not sufficiently protected, everyone will lose . . . it simply will be about how much one will lose, and when we will lose, both as individuals and as a society. At the same time, each party must also understand and accept that if privacy is also not sufficiently protected, everyone will also lose. This will become a question as to how much one will lose, as individuals and as a society. Truly accepting both positions as well as removing issues of distrust will lead to positive communication between the two entities, and will hopefully lead to a reasonable solution that both parties can accept. Is this possible? Yes. Is it likely? Who knows? What can be said is that if the parties are relying on litigation or new laws to resolve this dispute, it is possible one party will be pleased with that outcome; however, it is also possible that neither party will be pleased. Thus, it truly is in both parties' interests to work together to solve this dispute.